• ICT SECURITY

Scriptie

Afstudeeropdracht ICT security
Onderzoek en productselectie – SSL-VPN oplossingen

WESLEY VAN DER ZALM

1630301

VERSIE 0.14

Vakcode	:	TICT-AFSTUD-12
Versie	:	0.14
Startdatum	:	01-02-2016
Einddatum	:	31-05-2016
Naam student	:	Wesley van der Zalm
Studentnummer	:	1630301
E-mailadres	:	wesley.vanderzalm@student.hu.nl
Opdrachtgever	:	Bart Verhaar
Bedrijfsbegeleider	:	Simon van den Bos
Eerste examinator	:	Jos Snoeren
Docentbegeleider/Tweede examinator	:	Bert Buitenhuis

Versiebeheer

Versie	Datum	Wijzigingen
0.1	08-02-2016	- Eerste opzet scriptie: definiëren van de hoofdstukken.
0.2	10-02-2016	- Toevoegen van deelvragen en subdeelvragen.
0.3	11-02-2016	- Verwijderen van de teksten en de opbouw van het document aangepast voor een beter overzicht.
0.4	22-02-2016	- Het voorwoord geschreven en de verklarende woordenlijstabel, de hoofdvraag, de deelvragen, de subdeelvragen en de uitwerking van deelvraag 1 toegevoegd.
0.5	14-03-2016	- Uitwerkingen van het onderzoek toegevoegd.
0.6	05-04-2016	- Uitslag shortlist uitgewerkt en wijzigingen na leerteambijeenkomst verwerkt.
0.7	07-04-2016	- Uitwerkingen in de bijlage gezet.
0.8	11-04-2016	- Document doorlopen op spelling en grammatica.
0.9	20-04-2016	- Aanpassingen na feedback Bert Buitenhuis en Patrick ter Beek doorgevoerd.
0.10	02-05-2016	- Aanpassingen na feedback Melanie Groen doorgevoerd.
0.11	13-05-2016	- Verwerken van nieuwe resultaten en feedback Bert Buitenhuis.
0.12	23-05-2016	- Verwerken feedback Bart Verhaar. Voorwoord, Managementsamenvatting en conclusie toegevoegd.
0.13	25-05-2016	- Verder verwerken feedback Bart Verhaar. Grammatica en spelling verbeteren na feedback Melanie Groen.
0.14	26-05-2016	- Laatste feedback verwerken van Bart Verhaar na overleg.

Tabel 1 Versiebeheer

Distributielijst

Naam	Rol	Datum	Versie
Bert Buitenhuis	Docentbegeleider	11-02-2016	0.3
Simon van den Bos	Bedrijfsbegeleider	11-02-2016	0.3
Bart Verhaar	Opdrachtgever/mede-bedrijfsbegeleider	11-02-2016	0.3
Bert Buitenhuis	Docentbegeleider	11-04-2016	0.8
Patrick ter Beek	Student uit afstudeerleerteam	11-04-2016	0.8
Melanie Groen	Schrijvend journaliste	26-04-2016	0.9
Bert Buitenhuis	Docentbegeleider	09-05-2016	0.10
Simon van den Bos	Bedrijfsbegeleider	09-05-2016	0.10
Bart Verhaar	Opdrachtgever/mede-bedrijfsbegeleider	09-05-2016	0.10
Simon van den Bos	Bedrijfsbegeleider	18-05-2016	0.11
Bart Verhaar	Opdrachtgever/mede-bedrijfsbegeleider	18-05-2016	0.11
Melanie Groen	Schrijvend journaliste	24-05-2016	0.12
Bart Verhaar	Opdrachtgever/medebedrijfsbegeleider	25-05-2016	0.13

Tabel 2 Distributielijst

Voorwoord

Voor u ligt de scriptie ‘Onderzoek en productselectie – SSL-VPN oplossingen’. Deze scriptie is geschreven in het kader van mijn afstuderen aan de opleiding ‘System & Network engineering’ (SNE) aan de Hogeschool Utrecht in Utrecht. Van 1 februari 2016 tot en met 31 mei 2016 heb ik, Wesley van der Zalm, mijn afstudeeronderzoek gewijd aan de zoektocht naar een SSL VPN-oplossing voor Motiv en haar klanten. Dit onderzoek wordt uitgevoerd bij Motiv ICT Security te IJsselstein.

Steeds meer werknemers door heel Nederland maken gebruik van de mogelijkheid om thuis te werken. In 2012 werkte 32 procent van de werknemers zeker één dag per week thuis. Dit getal stijgt elk jaar weer. In 2015 is het aantal thuiswerkende werknemers naar 54 procent. Dit schrijft facto.nl die refereert naar jaarlijkse enquêtes met betrekking tot thuiswerken (Verbeek, 2015).

Telewerken kan positief of negatief uitpakken. Werknemers én werkgevers profiteren van vele voordelen als personeel vanuit huis werkt. Zo hebben werknemers minder last van files en hoeven werkgevers minder kantoorruimte te bewerkstelligen. Echter is de telewerker erg afhankelijk van de techniek. Wanneer de thuiswerkoplossing niet beschikbaar of gebruikersonvriendelijk is, leidt dit tot problemen. Daarnaast is het ook erg belangrijk dat data en gegevens worden beschermd (Eveleens, 2006).

De behoefte bij werknemers om mobiel te werken wordt steeds groter. Werknemers willen wanneer zij bijvoorbeeld gebruikmaken van een draadloos openbaar netwerk hun mail kunnen checken. Desalniettemin zijn er bij veel bedrijven angsten voor hackers of datalekken. Voor Motiv ligt hier de kans om een veilig, beheerde en mobiele werkomgeving aan te bieden. Gedurende mijn onderzoek heb ik mijn uiterste best gedaan om een passend antwoord te vinden op de vraag: *“Welke SSL-VPN oplossing past het beste bij de huidige eisen en wensen van Motiv en klanten?”*

Bij deze wil ik graag mijn bedrijfsbegeleiders (Bart Verhaar en Simon van den Bos) en docentbegeleider (Bert Buitenhuis) bedanken voor hun tijd, begeleiding en ondersteuning gedurende mijn afstudeerperiode.

Ik wens u veel leesplezier toe.

Wesley van der Zalm

IJsselstein, 7 april 2016.

Managementsamenvatting

In dit onderzoek wordt er gekeken of de huidige telewerkoplossing die Motiv aan haar klanten biedt nog voldoet aan de huidige eisen en wensen van Motiv en haar klanten. Ongeveer tien jaar geleden is er gekozen voor de telewerkoplossing van Juniper Pulse. De opdrachtgever wilt graag weten of deze oplossing aansluit bij de huidige marktvraag.

Aan het begin van dit onderzoek is onderzocht wat SSL VPN betekend en wat de verschillen zijn met IPSec VPN. Nadat er meer kennis was opgedaan over de techniek, zijn er korte interviews gehouden om de '*Key Criteria'* vast te stellen. Om een goed beeld te krijgen zijn er meerdere korte interviews gehouden om '*Key Criteria'* vanuit business-oogpunt en technisch-oogpunt te verzamelen. De '*Key Criteria'* zijn eisen waaraan een product moet voldoen. Wanneer er aan één '*Key Criteria'* niet voldaan werd, viel het product af. Deze methode van productselectie is gebaseerd op de KPMG pakketselectie methode (Hofland, 2009).

Vervolgens is er gekeken naar welke SSL-VPN oplossingen er op de markt zijn. Deze informatie is verstrekt door onder andere de Magic Quadrant van Gartner waarvan de laatste versie over dit onderwerp afkomstig is uit 2011 (Girard, 2011).

Naast de bekende producten die via Gartner zijn gevonden, zijn er ook producten onderzocht waar Motiv nieuwsgierig naar was. Dit bracht een totaal van veertien leveranciers op die werden getoetst aan de '*Key Criteria'*.

Van de veertien leveranciers zijn er zes doorgegaan naar de shortlist. Om eisen en wensen te verzamelen voor de shortlist is er een overleg ingepland bij Motiv. Gedurende dit overleg zijn er vragen gesteld om meer eisen en wensen boven tafel te krijgen. Door met meerdere personen dit overleg te voeren ontstond er de nodige interactie wat resulteerde in specifiekere eisen en wensen. Ook zijn er enquêtes afgenomen bij zes huidige klanten van Motiv. Deze enquêtes leverden eveneens weer extra eisen en wensen op.

Voor het prioriteren van eisen en wensen is gebruik gemaakt van de MoSCoW-methode (Osch, 2014). Dit heeft de weging van de uiteindelijke score per eis/wens bepaald.

Uit de shortlist zijn drie leveranciers naar voren gekomen die het beste scoorden, namelijk: Pulse Secure, Cisco en F5. De producten van deze leveranciers zijn ondervonden aan een *proof of concept*. Na het bouwen van de drie verschillende opstellingen zijn er verschillende testen uitgevoerd. Uit deze testen blijkt dat de oplossing van Pulse Secure het beste aansluit bij de huidige eisen en wensen van Motiv en haar klanten. Het product is het meest compleet en het eenvoudigst te beheren.

Dit onderzoek kan door Motiv gebruikt worden om de verschillen van hun huidige oplossing ten opzichte van andere oplossingen aan te tonen.

Inhoud

1.0 Inleiding

1.1 Introductie

Gedurende de periode van 1 februari 2016 tot en met 31 mei 2016 is er bij Motiv ICT Security onderzoek gedaan naar een SSL-VPN oplossing die voldoet aan de eisen en wensen van Motiv en klanten. Gedurende dit onderzoek is er naar een antwoord gezocht op de centrale onderzoekvraag:

"Welke SSL-VPN oplossing past het beste bij de huidige eisen en wensen van Motiv en haar klanten?"

De huidige oplossing die Motiv gebruikt en aanbiedt aan haar klanten wordt reeds tien jaar gebruikt. Door alle technologische veranderingen op het gebied van SSL-VPN oplossingen, de verschillende overnames en de nieuwe endpoints, zoals smartphones en tablets, vindt de opdrachtgever het belangrijk dat er onderzoek wordt gedaan naar welke oplossing op dit moment het beste aansluit. Voor Motiv is dit een buitengewone kans om hun dienst 'Veilig Telewerken' te verbeteren en meer informatie in te winnen over andere oplossingen die zich op de markt bevinden.

1.2 Leeswijzer

In dit document zijn alle bevindingen uit het onderzoek terug te lezen. Deze bevindingen leiden tot een conclusie. In de bijlagen zijn onder andere eerder opgestelde documenten te vinden.

- In hoofdstuk 1, de inleiding, vindt u een introductie over het onderwerp, een verklaring per hoofdstuk, een verklarende woordenlijst, informatie over de betreffende organisatie, de aanleiding en de kwestie met betrekking tot de opdracht, de doelstellingen, de belanghebbenden en de centrale onderzoeksvraag met bijhorende deelvragen en subdeelvragen.
- In hoofdstuk 2, de projectuitvoering, vindt u alle fasen van het project met een beschrijving. Per fase worden de op te leveren producten, de te behandelen deelvragen en de methoden beschreven.
- In hoofdstuk 3, resultaten en conclusies, vindt u de resultaten en antwoorden per deelvraag. Aan het eind van dit hoofdstuk, de conclusie, vindt u het antwoord op de centrale onderzoeksvraag. Afsluitend wordt er een advies aan Motiv geformuleerd.
- Hoofdstuk 4 bevat de bronvermeldingen van de scriptie, een lijst met gebruikte tabellen en figuren en de bijlagen.

1.3 Verklarende woordenlijst

In onderstaande tabel vindt u een lijst van begrippen die regelmatig terug komen in dit document. De afkortingen en begrippen worden in de tabel nader toegelicht.

Term	Toelichting
SSL	Afkorting voor 'Secure Socket Layer'. Dit protocol is bedoeld om veilig gegevens over het internet te versturen (Faura, 2005).
VPN	Afkorting voor 'Virtual Private Network'. Deze techniek maakt het mogelijk om vanaf een publiek netwerk een besloten/privé netwerk te benaderen (Faura, 2005).
TLS	Afkorting voor 'Transport Layer Security'. De vernieuwde versie van het SSL protocol. (Osman, 2008).
Telewerken	Werken tijdens werkuren op een andere locatie dan de arbeidsplaats, bijvoorbeeld vanuit huis (bestuurszaken.be, sd).
Endpoint	Een apparaat dat aan de gebruikerskant van het netwerk zit. Denk aan een pc, laptop, smartphone of tablet.
RDP	Afkorting voor 'Remote Desktop Protocol'. Dit protocol wordt gebruikt om een sessie op te zetten met een computer in een intern netwerk.
Radius	Staat voor 'Remote Authentication Dial In User Service'. Dit protocol wordt gebruikt voor authenticatie, autorisatie en accounting.
LDAP	Staat voor 'Lightweight Directory Access Protocol'.
HTML5	Staat voor 'HyperTekst Markup Language 5'. Deze versie is de vernieuwde versie van HTML die wordt gebruikt als 'opmaaktaal' voor het World Wide Web.
SSO	Staat voor 'Single Sign On'. Dit is een techniek die ervoor zorgt dat gebruikers eenmalig hoeven in te loggen.
SIEM	Staat voor 'Security Information and Event Management'. Dit is een systeem die gegevens uit het netwerk verzameld en meldingen (events) weergeeft.
ArcSight	De SIEM-oplossing van HP die bij Motiv wordt gebruikt.
Syslog	Een standaard die wordt gebruikt om logs te verzamelen.
SNMP	Staat voor 'Simple Network Management Protocol'. Dit protocol zorgt voor overdracht van informatie tussen netwerkapparaten.
Bookmarks	URL's die via een webbrowser benaderbaar zijn.
Key criteria	De vereisten of voorwaarden voor een oplossing.
Firewall	Een systeem dat zorgt voor bescherming van buitenaf.
MSP	Managed Services Provider. Een model die zorgt voor kortingen bij grotere afname.
Proof of concept	Het bouwen, testen en presenteren van een testopstelling.
Moscow-methode	Een wijze van prioriteren waar de medeklinkers uit het woord 'Moscow' symbool staan voor een prioriteit.
IPSec	Een standaard die gebruikt wordt voor het beveiligen van het Internet Protocol (IP) doormiddel van authenticatie en encryptie.
Authentication Header	Eén van de twee belangrijkste headers binnen het IPSec protocol.
Encapsulating Security Payload	Eén van de twee belangrijkste headers binnen het IPSec protocol.

Internet Security Agreement/Key Management Protocol	Afgekort ISAKMP, zorgt ervoor dat twee computers akkoord gaan met bepaalde security instellingen om vervolgens een beveiligde sleutel uit te wisselen voor veilige communicatie
Intrusion Prevention System	Een systeem dat verdachte pakketten dropt (weggooit). Een Intrusion Prevention System kan de content van elk IP-pakket controleren om te bepalen of er een aanval aan de gang is.
Intrusion Detection System	Een systeem dat hackpogingen en ongeautoriseerde toegang tot een netwerk of systeem detecteert.
Role based access control	De rol van een gebruiker bepaald hoeveel en welke toegangen er zijn tot het netwerk.

Tabel 3 Verklarende woordenlijst

1.4 Organisatie opdrachtgever

Motiv is een ICT-security organisatie die andere organisaties voorziet van IT-beveiligingsoplossingen en -diensten. Deze maatregelen zijn nodig ter voorkoming van cybercriminaliteit, datadiefstal en datalekken. Motiv levert al sinds 1998 security-oplossingen vanuit de disciplines netwerk- en security-infrastructuur, consultancy, applicatieontwikkeling en databasetechnologie. Motiv biedt een breed scala aan 24x7 Managed Security Services en hosting. Door het eigen Security Operations Center worden cyberaanvallen, kwetsbaarheden en datalekken opgespoord, voorkomen en beperkt.

Motiv is gevestigd in IJsselstein en heeft ca. 110 medewerkers. Motiv's bedrijfsprocessen, softwareontwikkeling en Managed Security Services zijn gecertificeerd op basis van ISO9001 (kwaliteitsmanagement), ISO27001 (informatiebeveiliging) en ISO20000 (Service Management op basis van ITILv3).

1.5 Aanleiding en kwestie

De laatste jaren is het SSL-VPN landschap stevig veranderd. Zo wordt bijvoorbeeld steeds vaker een telewerkoplossing gecombineerd met andere security oplossingen, zoals firewalls, op één systeem. Tegenwoordig willen steeds meer gebruikers een VPN verbinding maken met apparaten als smartphones en tablets. Motiv is op zoek naar een veilige SSL-VPN oplossing die goed past bij de nieuwe eisen en wensen die voort zijn gekomen uit de nieuwe veranderingen. De opdrachtgever wilt de resultaten van deze opdracht kunnen gebruiken om een keuze voor een oplossing te maken.

In het verleden (ongeveer 10 jaar geleden) is gekozen voor Juniper Pulse als VPN oplossing binnen het portfolio van Motiv. Juniper Pulse wordt geleverd als product of dienst tegen een vast bedrag per gebruiker per maand. Motiv kent daarnaast de volgende beheerdiensten:

- Easy Connect: de klant is verantwoordelijk voor de security. Motiv zorgt voor (product)ondersteuning;
- Service Connect: het technische IT beheer van de dienst wordt volledig of gedeeltelijk door Motiv uitgevoerd. Er wordt geen beveiligingsbeheer verzorgt door Motiv;
- Full Connect: het technische IT beheer en het beveiligingsbeheer van de dienst wordt volledig door de beveiligingsexperts van Motiv uitgevoerd (Bastiaan Bakker, 2014).

Momenteel heeft Motiv ongeveer 10 klanten in volledig beheer.

Door de jaren heen is er echter een hoop veranderd. Zo zijn er nieuwe typen endpoints bijgekomen, worden VPN oplossingen anders geïmplementeerd en zijn er verschillende overnames geweest. Motiv ziet deze opdracht als een kans om de dienst 'Veilig Telewerken' meer onder de aandacht te kunnen brengen. Steeds vaker zoeken klanten zelf naar een oplossing. Motiv is daarom op zoek naar een oplossing die de dienst 'Veilig Telewerken' uniek maakt en ervoor zorgt dat de dienst aansluit bij de huidige marktvraag.

1.6 Doelstellingen

Het doel is om aan de hand van de gestelde eisen en wensen een productselectie te maken en de best scorende oplossingen te testen in een lab opstelling. Uiteindelijk worden er naast de huidige oplossing één of twee vernieuwde oplossingen gebouwd in een testomgeving (*proof of concept*). Het aantal gekozen oplossingen hangt af van de uiteindelijke score ten opzichte van de eisen en wensen. Wanneer een vernieuwde oplossing hoger scoort dan de rest, is het niet langer nodig om een andere oplossing te bouwen.

Uiteindelijk wordt er aan de hand van een *proof of concept* een keuze gemaakt door de student. Deze keuze zal worden gebaseerd op uitslagen uit het gehele onderzoek. De oplossing die het best scoort op de test zal worden gekozen. De keuze kan eveneens vallen op de huidige oplossing van Motiv.

De gekozen oplossing wordt gepresenteerd aan Motiv in een eindpresentatie. In de eindpresentatie wordt uitgelegd waarom deze oplossing de beste keuze is voor Motiv en haar klanten en hoe ik tot die keuze ben gekomen. Het doel van de opdracht is om een advies over welke oplossing het beste bij de eisen en wensen past aan Motiv te geven. De productmanager van Motiv en tevens opdrachtgever (Bart Verhaar) wil aan de hand van mijn onderzoek een keuze kunnen maken voor het beste product.

De opdracht is voltooid wanneer er een goed onderbouwd advies kan worden gegeven aan de opdrachtgever. Om dicht bij de kern te blijven, is er in overleg besloten dat cloud-oplossingen buiten beschouwing worden gelaten gedurende het project.

1.7 Belanghebbenden

De volgende personen hebben belang bij de uitkomst van het onderzoek:

Aksel Dorèl
Algemeen directeur Motiv

Simon van den Bos
Opdrachtgever en bedrijfsbegeleider Motiv

Bart Verhaar
Mede-bedrijfsbegeleider en productmanager Motiv

Bert Buitenhuis
Docentbegeleider namens Hogeschool Utrecht

Wesley van der Zalm
Als student verantwoordelijk voor de uitvoering van de opdracht

1.8 Centrale onderzoeksvraag, deelvragen en subdeelvragen

In onderstaande tabellen vindt u de hoofdvraag die centraal staat in dit onderzoek (tabel 4) en de bijhorende deelvragen en subdeelvragen (tabel 5). Deze vragen worden uitgewerkt in hoofdstuk 3: 'Resultaten en conclusies'.

Hoofdvraag:
Welke SSL-VPN oplossing past het beste bij de huidige eisen en wensen van Motiv en haar klanten?

Tabel 4 Hoofdvraag

Nr.	Deelvraag	Nr.	Subdeelvraag
1	Wat zijn de verschillende tussen SSL VPN en IPSec VPN en welke '*Key Criteria*' stellen Motiv en haar klanten aan een SSL-VPN oplossingen?	1.1	Hoe werkt SSL VPN en IPSec VPN en wat zijn de grootste verschillen?
		1.2	Wat zijn de '*Key Criteria*' vanuit business en technisch oogpunt?
		1.3	Welke SSL-VPN oplossingen zijn er op de markt?
		1.4	Hoe scoren de voorgeselecteerde SSL-VPN oplossingen op de vastgestelde '*Key Criteria*'?
2	Wat zijn de eisen en wensen van Motiv en haar klanten en hoe belangrijk zijn deze?	2.1	Welke vragen moeten er aan wie gesteld worden om de eisen en wensen te bepalen?
		2.2	Wat zijn de eisen en wensen van Motiv en haar klanten?
		2.3	Hoe belangrijk zijn de eisen en wensen van Motiv en haar klanten?
3	Welke twee oplossingen scoren het beste op de vastgestelde eisen en wensen?	3.1	Hoe wordt de score van de oplossingen bepaald?
		3.2	Hoe scoren de oplossingen uit de longlist op de vastgestelde eisen en wensen?
4	Hoe zien de geselecteerde en de huidige SSL-VPN oplossingen er in een testomgeving uit?	4.1	Hoe ziet het technisch en functioneel ontwerp van de huidige SSL-VPN oplossing er uit?
		4.2	Hoe zien de technisch en functioneel ontwerpen van de geselecteerde SSL-VPN oplossingen er uit?
		4.3	Wat is er nodig om de SSL-VPN oplossingen op te zetten in een testomgeving?
		4.4	Hoe zijn de testopstellingen geconfigureerd?
5	Hoe scoren de SSL-VPN oplossingen in een testomgeving?	5.1	Waar moeten de testopstellingen op worden getest?
		5.2	Hoe ziet het resultaat van de test er per opstelling uit?

Tabel 5 Deelvragen en subdeelvragen

2.0 Projectuitvoering

Het afstudeerproject is verdeeld over verschillende fasen. Per fase wordt er een toelichting gegeven over de gebruikte methoden en eventueel de bijbehorende deelvragen. De fasen uit dit project bestaan uit:

1. Voorbereiding
2. Analyse en onderzoek
3. Productselectie
4. Bouwen en testen
5. Oplevering

2.1 Voorbereiding

Onder de voorbereiding valt het verwerven van een afstudeeropdracht. Na meerdere sollicitaties en gesprekken is de keuze gevallen op Motiv ICT Security in IJsselstein. Deze keuze is gebaseerd op de mensen waarmee ik contact heb gehad en door het beoordelen van de (type) opdracht.

Gedurende de voorbereiding zijn er twee afspraken bij Motiv geweest. Het eerste gesprek was een sollicitatie en een stukje bespreking van de opdracht. Aan de hand van dit gesprek is er een eerste versie van het afstudeervoorstel geschreven. Gedurende het schrijven zijn er punten open gebleven die nog eens nagevraagd moesten worden. Hiervoor is nogmaals een afspraak gemaakt met Simon van den Bos. In januari 2016 is het afstudeervoorstel goedgekeurd.

Voorbereiding	
Op te leveren producten:	Afstudeervoorstel
Behandelde deelvragen:	N.V.T.
Gebruikte methoden:	- Documentatie aan de hand van het boek ‘Leren communiceren’ (Steehouder, 2012)

Tabel 6 Projectuitvoering voorbereiding

2.2 Analyse en onderzoek

De fase ‘analyse en onderzoek’ begint met een bedrijfsoriëntatie. Dit betekent een kennismaking met de medewerkers en uitleg van Iris Swartjes (HR Manager) over het gebouw, de afdelingen en de regels binnen het bedrijf.

De eerste weken van aanwezigheid bij Motiv is er veel deskresearch gedaan om meer te weten te komen over het onderwerp van de opdracht. Vragen die ik mezelf stelden waren bijvoorbeeld:

- Hoe werkt een SSL-VPN oplossing precies?
- Welke eisen zouden er gesteld kunnen worden aan een SSL-VPN oplossing?
- Hoe werkt de huidige SSL-VPN oplossing?

In dezelfde periode ben ik aan de slag gegaan met het schrijven van mijn plan van aanpak en is er een gesprek geweest met Bert Buitenhuis, Simon van den Bos en Bart Verhaar.

Analyse en onderzoek		
Op te leveren producten:	-	Plan van Aanpak
Behandelde deelvragen:	N.V.T.	
Gebruikte methoden:	-	Deskresearch
	-	Literatuuronderzoek
	-	Documentatie aan de hand van het boek 'Leren communiceren' (Steehouder, 2012)

Tabel 7 Projectuitvoering analyse en onderzoek

2.3 Productselectie

Als het afstudeercontract is getekend, kan er begonnen worden aan de opdracht. Deze fase staat in het teken van het beantwoorden van de deelvragen die worden benoemd in tabel 8. Deze vragen zijn opgesteld in het plan van aanpak dat is goedgekeurd door het tekenen van het afstudeercontract.

Om de eerste vraag te beantwoorden, zijn er interviews afgenomen binnen Motiv. Bart Verhaar en Simon van den Bos formuleerden de business criteria en Fabian Gugelot formuleerde de technische criteria. Door het vooronderzoek en aan de hand van Gartner's Magic Quadrant zijn er verschillende leveranciers geselecteerd. De '*Key Criteria*' zijn hier tegen afgewogen en er is een selectie gemaakt.

De leveranciers die overblijven na de voorselectie worden verder onderzocht in de shortlist. Dit betekent dat er per leverancier een score per eis of wens wordt bepaald. De eisen en wensen zijn voortgekomen uit een overleg met Bart Verhaar, Simon van den Bos en Fabian Gugelot. Daarnaast zijn er enquêtes afgenomen bij zes huidige klanten van Motiv. De eisen en wensen zijn geprioriteerd aan de hand van de MoSCoW-methode. Aan de hand van deze prioriteit is een weging bepaald.

Productselectie		
Op te leveren producten:	-	Ingevulde longlist
	-	Ingevulde shortlist
Behandelde deelvragen:	-	Wat zijn de '*Key Criteria*' van Motiv en haar klanten en welke SSL-VPN oplossingen voldoen daaraan?
	-	Wat zijn de eisen en wensen van Motiv en haar klanten en hoe belangrijk zijn ze?
	-	Welke twee oplossingen scoren het beste op de vastgestelde eisen en wensen?
Gebruikte methoden:	-	Interviews
	-	KPMG-pakketselectiemethodiek
	-	MoSCoW-methode
	-	Documentatie aan de hand van het boek 'Leren communiceren' (Steehouder, 2012)

Tabel 8 Projectuitvoering productselectie

2.4 Bouwen en testen

Na het selecteren van één of twee vernieuwde oplossingen dient er een technisch ontwerp gemaakt te worden. Deze is nodig om goedkeuring te krijgen voor het opzetten van het *proof of concept* (PoC) in het lab van Motiv. Voor het bouwen moet er een testplan zijn, zodat de testopstellingen getest kunnen worden.

Bouwen en testen	
Op te leveren producten:	- Technische ontwerp - Testrapport
Behandelde deelvragen:	- Hoe zien de geselecteerde en de huidige SSL-VPN oplossingen er in een testomgeving uit? - Hoe scoren de SSL-VPN oplossingen in een testomgeving?
Gebruikte methoden:	- Testplan template van de ASL BiSL foundation (ASL BiSL Foundation, 2006)

Tabel 9 Projectuitvoering bouwen en testen

2.5 Oplevering

De fase 'oplevering' betekent het afronden van het project. In deze fase wordt de scriptie afgerond en nagekeken. Er wordt een presentatie voorbereid die plaatsvindt bij Motiv. Vervolgens wordt deze presentatie tevens op school gegeven tijdens de afstudeerhoorzitting.

Oplevering	
Op te leveren producten:	- Scriptie - Presentatie
Behandelde deelvragen:	Alle, inclusief de hoofdvraag van het onderzoek
Gebruikte methoden:	- Documentatie aan de hand van het boek 'Leren communiceren' (Steehouder, 2012)

Tabel 10 Projectuitvoering oplevering

3.0 Resultaten en conclusies

3.1 De werking van en de verschillen tussen SSL VPN en IPSec VPN

Om de vraag “Wat zijn de verschillende tussen SSL VPN en IPSec VPN en welke ‘*Key Criteria*’ stellen Motiv en haar klanten aan een SSL-VPN oplossingen?” te kunnen beantwoorden, is het noodzakelijk om eerst de kenmerken van SSL VPN en IPSec VPN te kennen. Aan de hand daarvan zijn vragen opgesteld die nodig zijn om de ‘*Key Criteria*’ te bepalen. Hiermee worden de harde eisen bedoeld waaraan een oplossing minimaal moet voldoen. Deze eisen moeten duidelijk worden na interviews met Bart Verhaar (Productmanager Motiv) en Simon van den Bos (Bedrijfsbegeleider bij Motiv) voor de business gerelateerde eisen en met Fabian Gugelot (Security Engineer Motiv) en diensteigenaar van de dienst ‘Veilig telewerken’ voor de technische eisen.

Als de eisen voor een oplossing bekend zijn, kan er onderzoek gedaan worden naar de producten op de markt die voldoen aan de vastgestelde eisen. Uit dit onderzoek volgt een longlist die het antwoord geeft op deze deelvraag.

3.1.1 De werking van SSL

SSL (Secure Socket Layer) is een beveiligingsprotocol dat veel gebruikt wordt bij internet communicatie. Een Functie van het SSL protocol is bijvoorbeeld het beveiligen van HTTP. Het SSL protocol zorgt op drie manieren voor een veilige verbinding:

- Privacy: zorgt voor een encryptie van de verbinding;
- Identiteit authenticatie: identificatie aan de hand van certificaten;
- Betrouwbaarheid: er wordt een integriteitscontrole uitgevoerd op de berichten.

Het SSL protocol bestaat uit vier protocol lagen, namelijk: Record Layer, ChangeCipherSpec Protocol, Alert Protocol en Handshake Protocol (McKinley, 2003).

De twee belangrijkste protocollen binnen het SSL protocol zijn de Handshake Protocol en de Record Layer (Pillai, 2003).

Om een SSL verbinding tot stand te brengen, wordt er als eerste de handshake uitgevoerd. Als eerst stuurt de client een ‘Client hello’ bericht naar de server. Ook stuurt de client zijn SSL versie en Cipher informatie. Als de server deze berichten heeft ontvangen, wordt er een ‘Server hello’ bericht teruggestuurd. Ook stuurt de server de CipherSuite en het servercertificaat. Optioneel kan er worden gevraagd naar een client certificaat.

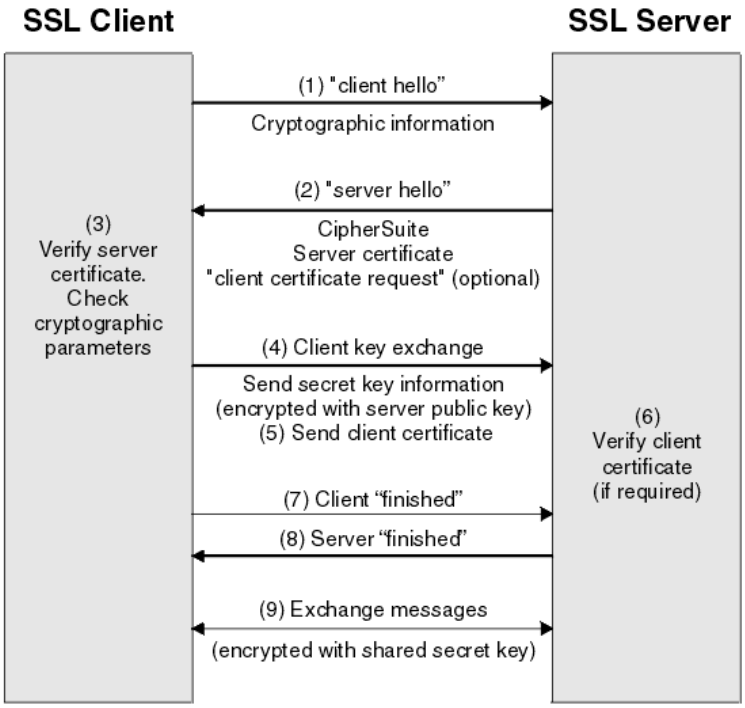
De client verifieert vervolgens dat het systeem communiceert met de juiste server. Dit doet de client door onder andere de digitale handtekening te controleren. Wanneer de server is geïdentificeerd, stuurt de client een willekeurige reeks (string) van bytes die wordt gebruikt om de ‘secret key’ van de client en server te berekenen. Deze reeks is versleuteld met de ‘public key’ van de server.

Wanneer de server een ‘client certificate request’ heeft gedaan, stuurt de client wederom een willekeurige reeks bytes (versleuteld met de ‘secret key’ van de client), inclusief het certificaat van de client of een ‘no digital certificate alert’. In het geval van een alert geldt dit als een waarschuwing voor de server. Soms zorgt dit ervoor dat de handshake mislukt. (An overview of the SSL or TLS handshake, 2014). Als de server het certificaat wel heeft ontvangen, wordt deze door de server geverifieerd.

De client stuurt een ‘finished’ bericht die versleuteld is met de ‘secret key’. Met dit bericht laat de client aan de server weten dat de handshake voor de client is gelukt. De server doet vervolgens hetzelfde en stuurt het ‘finished’ bericht naar de client.

De sessie is nu tot stand gebracht. De client en server communiceren met elkaar via symmetrische encryptie. Ze maken dus beide gebruik van dezelfde ‘shared secret key’ (An overview of the SSL or TLS handshake, 2014).

In figuur 1 zijn de stappen van de handshake nog eens te zien.



Figuur 1 SSL handshake (An overview of the SSL or TLS handshake, 2014)

3.1.2 De werking van IPSec

IPSec (Internet Protocol Security) is een verzameling van protocollen die zorgen voor beschermde communicatie over IP netwerken. De verschillende protocollen werken samen in verschillende combinaties om de communicatie te beschermen. IPSec wordt voornamelijk voor VPN gebruikt (Sheila Frankel K. K., 2005).

Een aantal componenten vormen het pakket 'IPSec'. Deze standaard valt op te splitsen in twee belangrijke headers die het werk voor het IPSec protocol doen. De twee belangrijkste headers zijn de Authentication Header (AH) en de Encapsulating Security Payload (ESP). Om hun taken uit te voeren maken deze twee headers gebruik van andere protocollen en services (Kozierok, 2005).

Het Internet Security Agreement/Key Management Protocol (ISAKMP) zorgt ervoor dat twee computers akkoord gaan met bepaalde security instellingen om vervolgens een beveiligde sleutel uit te wisselen voor veilige communicatie. Een Security Association (SA) zorgt ervoor dat alle informatie verzameld wordt om veilig te kunnen communiceren. De SA bevat policy agreements die controleren op welke algoritmes, key lengte en bestaande beveiligingssleutel er gebruikt wordt door deze twee machines.

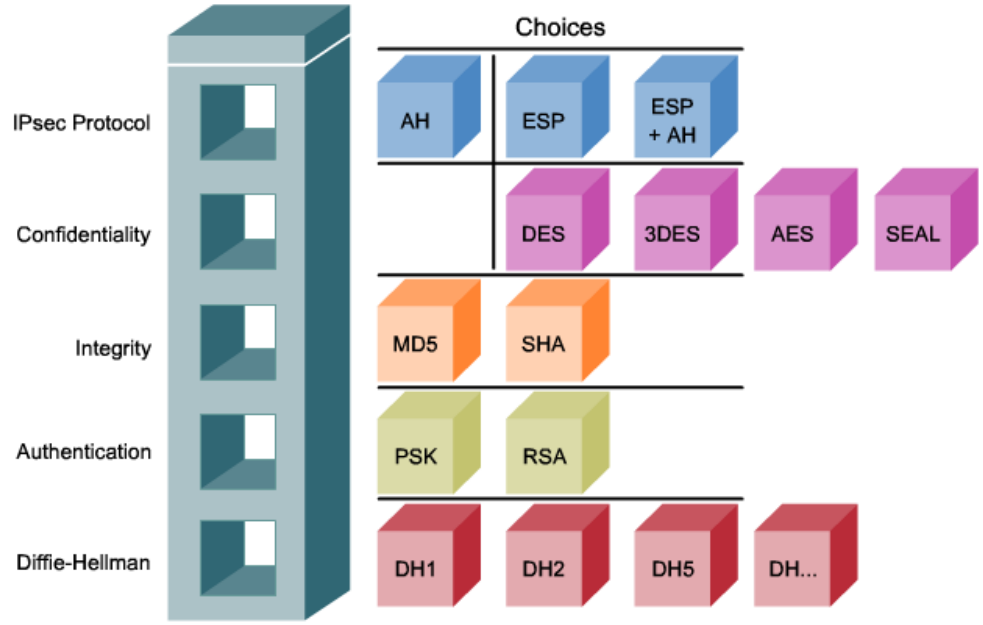
Dit proces bestaat uit de volgende stappen:

1) Het eens worden over het te gebruiken encryptiealgoritme.
2) Het eens worden over het algoritme bij het verifiëren van berichtcontrole.
3) Bepalen hoe de verbinding geauthentiseerd wordt. Dit kan door gebruik van public-key certificate, een shared secret key of Kerberos.
4) Bepalen of de AH gebruikt gaat worden.
5) Bepalen of de ESP gebruikt gaat worden.
6) Bepalen welk encryptiealgoritme er gebruikt wordt voor ESP.
7) Bepalen welk authenticatieprotocol er gebruikt wordt voor AH.

Om een veilige verbinding te maken over het publieke netwerk wordt er minimaal één en maximaal twee van de mechanismen (AH en ESP) gebruikt (Firewall.cx, sd).

De Authentication Header wordt afgeraden voor telewerken over het publieke netwerk, omdat deze vorm van IPSec de informatie niet versleuteld (Govcert.nl, 2009).

In figuur 2 staat het IPSec framework afgebeeld. Hier is goed te zien dat het IPSec protocol een verzameling van protocollen is. Voor alle kenmerken van IPSec is er een keuze uit verschillende protocollen. Ook is te zien wanneer er alleen voor de Authentication Header wordt gekozen, er geen sprake is van vertrouwelijkheid (Confidentiality).



Figuur 2 IPSec Architecture (Padam Gurung, 2014)

3.1.3 De werking van SSL VPN

SSL VPN maakt gebruik van de opvolger van SSL, namelijk TLS (Transport Layer Security). TLS is gebaseerd op de werking van het SSL protocol.

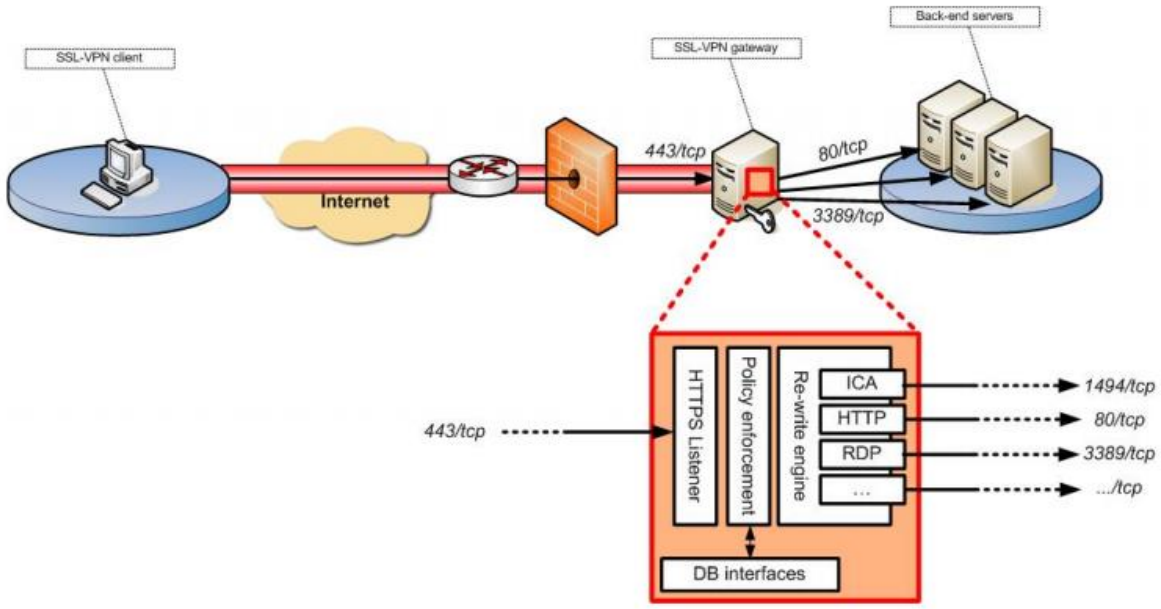
Wanneer een gebruiker een VPN sessie start vanuit de webbrowser, gebeurt dat niet via het HTTP protocol op poort 80, maar wordt er een beveiligde verbinding gemaakt op poort 443 met het protocol HTTPS (HTTP in combinatie met SSL). Ook webmail kan via een HTTP of HTTPS sessie via de webbrowser worden benaderd. Webbased applicaties worden ondersteund door alle moderne browsers. Dit zorgt ervoor dat gebruikers gemakkelijk hun applicaties kunnen benaderen via een smartphone, tablet, laptop, pc of MAC (OpenReach, 2002).

Omdat alle communicatie via HTTPS gaat, wordt deze oplossing ook wel ‘HTTPS VPN’ of ‘HTTP over SSL VPN’ genoemd. Via de webbrowser kan de gebruiker inloggen op een webportal. Als de sessie tot stand is gekomen, krijgt de gebruiker een keuzemenu van applicaties waar hij recht op heeft. Er is alleen ondersteuning voor applicaties die HTTP ondersteunen. Gebruikers hoeven hier geen software voor te installeren. Enkele voorbeelden van applicaties die te benaderen zijn via de webportal:

- E-mail (in de vorm van webmail)
- File shares
- Web (bijvoorbeeld een intranetpagina)
- Virtuele desktops (Citrix, Vmware of Remote Desktop)

Omdat SSL VPN makkelijker te gebruiken is en op meer plekken toegang biedt, is SSL VPN de beste oplossing voor gebruikers die toegang willen tot het bedrijfsnetwerk (OpenReach, 2002).

Applicaties die geen HTTP ondersteunen kunnen alleen op een speciale manier worden benaderd. Hiervoor zijn wel een software-installatie en Administrator-rechten vereist (Govcert.nl, 2009).



Figuur 3 SSL VPN infrastructuur (Govcert.nl, 2009)

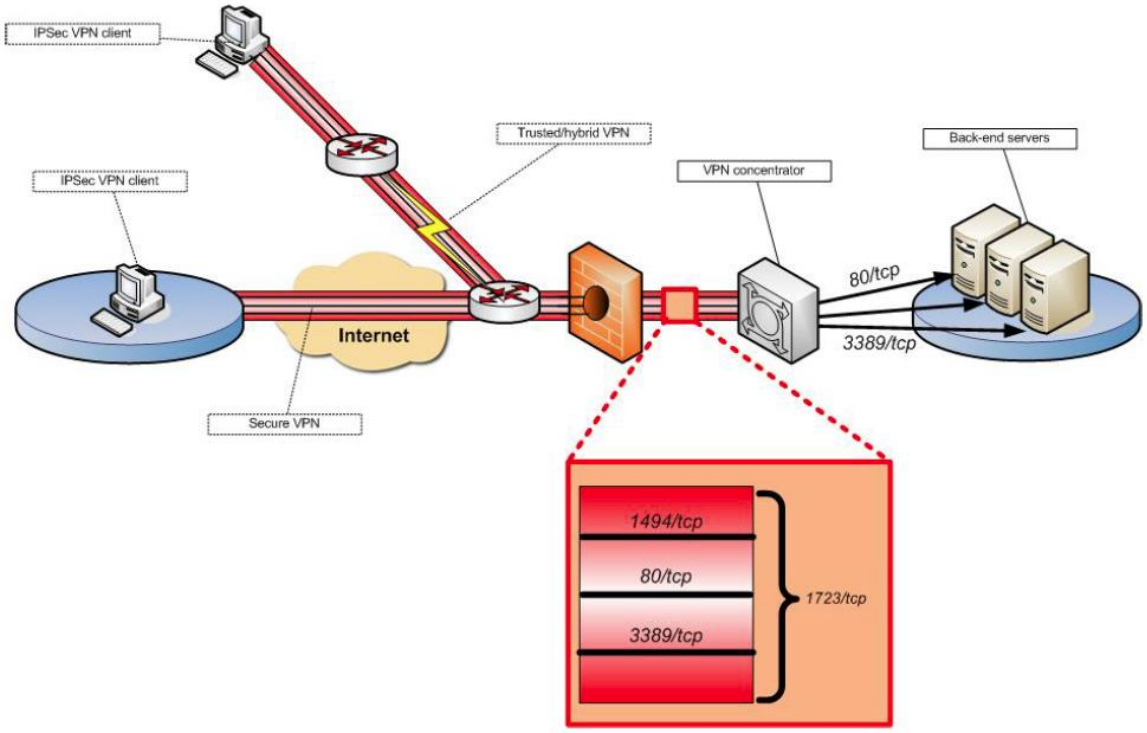
3.1.4 De werking van IPSec VPN

Gebruikers die een VPN sessie willen starten via IPSec, dienen dat via client-software van de leverancier te doen.

Wanneer gebruikers een IPSec VPN verbinding maken met een (bedrijfs)netwerk, hebben zij client software nodig. Deze software dient ook juist geconfigureerd te worden. Voor niet-technische gebruikers kan dit problemen opleveren. Het voordeel van IPSec is dat de standaard bescherming biedt tussen twee endpoints en alle applicaties op de netwerklaag. Voor gebruikers lijkt het net alsof ze op kantoor aanwezig zijn, omdat ze dezelfde toegang hebben als op het werk. Denk hierbij aan:

- E-mail
- File share
- Web (HTTP)
- Client-server
- Databases
- Terminal services

Om deze reden is IPSec VPN de beste oplossing voor toegang op bijkantoren.



Figuur 4 IPSec VPN infrastructuur (Govcert.nl, 2009)

3.1.5 Kenmerken en verschillen van IPSec VPN en SSL VPN

In onderstaande tabel (tabel 11) worden de verschillen tussen IPSec VPN en SSL VPN nog eens duidelijk naast elkaar gezet. Het is duidelijk af te lezen dat SSL VPN meer toegankelijkheden biedt voor gebruikers. Dit komt omdat een verbinding opzetten gemakkelijker is en met meer apparaten mogelijk is. Tevens is het een optie om klanten beperkte toegang te geven.

	IPSec VPN	SSL VPN
Client	IPSec VPN Client	Webbrowser of SSL VPN Client software
Toegangsbeveiliging	Basis (host- en poortniveau)	Uitgebreid (URL/URI gebaseerd)
Doelgroep	Interne medewerkers	Interne medewerkers en klanten (extranetten)
Applicaties	Toegang tot alle applicaties	Alleen webbased applicaties zoals webmail, intranet, fileshares en virtuele desktops
Verbindingsopties	Alleen specifieke apparaten met specifieke configuratie	Elke apparaat met een internetverbinding en een webbrowser
OSI-laag	Netwerk (laag 3)	Applicatie (laag 7), Presentatie (laag 6) en Transport (laag 4)

Tabel 11 Kenmerken IPSec VPN en SSL VPN

3.1.6 Vastgestelde '*Key Criteria*' en leveranciers

Om een eerste selectie te maken van SSL-VPN oplossingen, zijn er '*Key Criteria*' nodig. De '*Key Criteria*' vanuit business oogpunt zijn voortgekomen uit een gesprek met Bart Verhaar (Productmanager Motiv). Na het gesprek is onderstaande tabel opgesteld en bevestigd door Bart Verhaar (zie bijlage 5).

In onderstaande tabel staan de harde eisen voor een oplossing met daarbij de opgegeven reden.

Key criteria	Reden
Ondersteuning van Radius, LDAP, SAML	Protocollen die nodig zijn voor de authenticatie van gebruikers.
Ondersteuning van minimaal de volgende besturingssystemen: Mac OSX, iOS, Android, Windows 7, Windows 8 en Windows 10.	Betreft de meest gebruikte Operating systemen van Motiv en klanten.
Mogelijkheid voor multi-tenancy	Klanten moeten gescheiden beheerd kunnen worden.
Maximaal éénmalig lokale administratorrechten nodig voor het installeren van client-software.	Wanneer klanten bij elke update lokale administratorrechten nodig hebben, gaat dit voor veel gebruikersproblemen zorgen.
Minimaal ondersteuning voor: RDP, Citrix VDI (ICA) en VMware VDI (PCoIP)	Om virtuele machines via de VPN oplossing te kunnen benaderen. Een deel van de huidige klanten gebruikt hiervoor de Citrix oplossing en een ander deel de VMware oplossing. Beide typen virtuele desktops moeten dus ondersteund worden door een nieuwe oplossing.

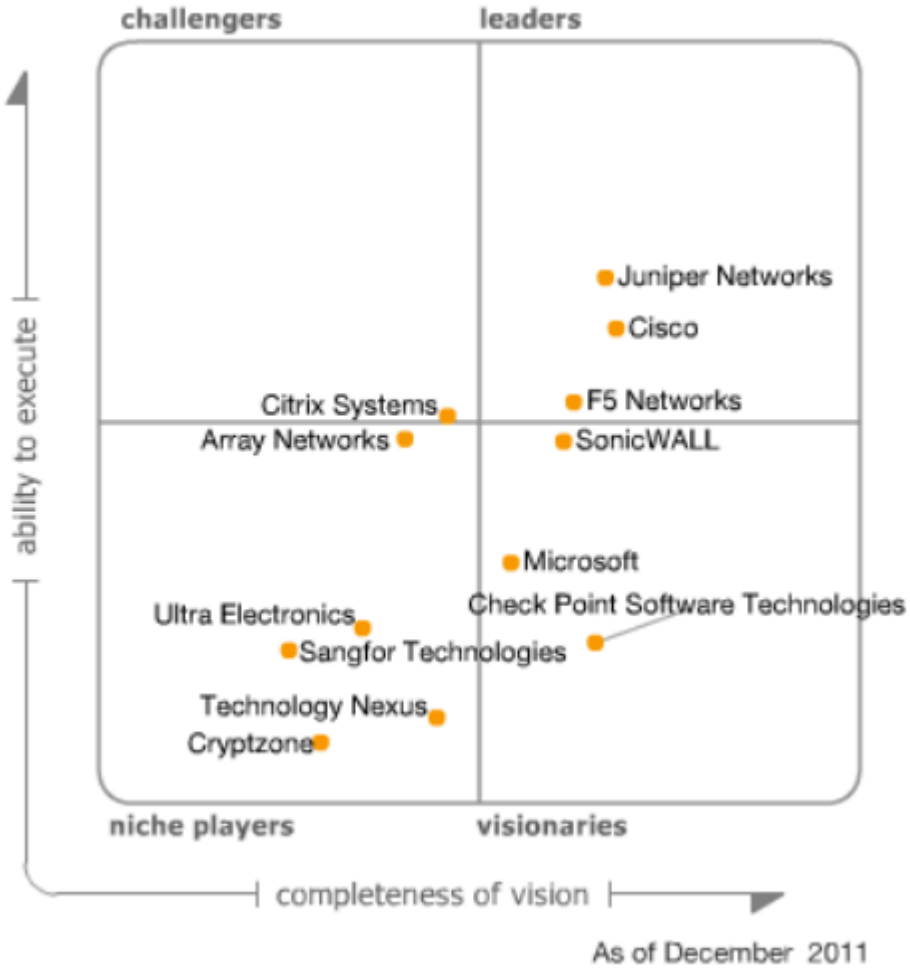
Tabel 12 Vastgestelde 'Key Criteria' vanuit business oogpunt

In tabel 13 zijn de technische '*Key Criteria*' te lezen die zijn vastgesteld aan de hand van een gesprek met Fabian Gugelot. Ook deze zijn per email bevestigd (zie bijlage 5).

Key Criteria	Reden
Mogelijkheid voor toekennen van bookmarks	Als gebruikers inloggen moeten ze bookmarks te zien krijgen, wanneer ze hier recht op hebben. Denk bijvoorbeeld aan fileshares (FTP), Terminal Services (RDP) via ActiveX of Java en voor beheerders aan SSH en Telnet.
Kan VPN tunneling	Om veilig toegang te geven tot verschillende netwerk services.
Beschikt over een Host-checker	Om devices van gebruikers eerst te kunnen controleren op bepaalde voorwaarden en aan de hand daarvan bepaalde resources te geven. Denk bijvoorbeeld aan up-to-date antivirus software.
Ondersteund SNMP, Syslog en Koppeling HP ArcSight (SIEM) voor monitoring	SNMP en Syslog gegevens wordt naar de HP ArcSight SIEM oplossing gestuurd om de SSL VPN oplossing te kunnen monitoren.
Moet minimaal één van de volgende authenticatie-methode bevatten m.b.t. SSO: - Kerberos protocol - Basic authenticatie - NTLM protocol - Remote authenticatie	Door gebruik te maken van de Single Sign On techniek hoeven gebruikers maar één keer in te loggen. Deze techniek wordt in de huidige situatie in combinatie met sterke authenticatie al gebruikt en moet worden behouden.
Ondersteuning voor HTML5	Browsers die HTML5 ondersteunen bieden meer functionaliteit, zoals de opties om meer elementen te openen zonder plug-ins, het weergeven van video's en afspelen van audiofragmenten. Een SSL-VPN oplossing moet hier ook aan voldoen.
Er moet een mogelijkheid zijn om alleen SSL VPN te gebruiken (webbased en clientless)	Gebruikers moeten minimaal toegang hebben tot het bedrijfsnetwerk zonder software te hoeven installeren.

Tabel 13 Vastgestelde 'Key Criteria' vanuit technisch oogpunt

Uit een voorselectietraject zijn veertien leveranciers naar voren gekomen. Deze selectie is gebaseerd op onderzoek via internetbronnen, tips van mijn bedrijfsbegeleider en Gartners Magic Quadrant (figuur 5).



Figuur 5 Magic Quadrant for SSL VPN's (Girard, 2011)

Uit de Magic Quadrant zijn de leaders en visionaries meegenomen naar de longlist. In dit geval dus Juniper Networks (tegenwoordig Pulse Secure), Cisco, F5 Networks, Sonicwall en Check Point. De laatste Magic Quadrant dateert van 2011. De overige leveranciers op de longlist zijn voortgekomen vanuit Motiv. Motiv wil graag Citrix, Palo Alto, Netmotion en Fortinet onderzocht hebben (Fabian Gugelot, 2016). Daarnaast wil Motiv minder bekende oplossingen in het onderzoek meenemen. Hiervoor zijn Sangfor, Cryptzone, WatchGuard, Array Networks en Barracuda onder de loep genomen.

In onderstaande tabel (tabel 14) vindt u de uitslag van de longlist waar alle leveranciers zijn onderzocht op cruciale punten. Per functie wordt er aangegeven of de leveranciers wel of niet voldoen. De gestelde eisen zijn ’Must haves‘ voor een oplossing. Alleen de leveranciers die aan alle eisen voldoen, worden verder meegenomen in het selectietraject en worden verder onderzocht in de shortlist.

Key Criteria/Leverancier	WatchGuard	Dell	F5 Networks	Barracuda	Cisco	Check Point	Pulse	Citrix	Sangfor	Cryptzone	Fortinet	Palo Alto	Array Networks	Netmotion
Radius, LDAP, SAML	V	V	V	V	V	V	V	V	V	V	V	V	V	V
Ondersteuning van minimaal de volgende besturingssystemen: Mac OSX, iOS , Android, Windows 7, Windows 8 en Windows 10	X	V	V	V	V	V	V	V	V	V	V	V	V	V
Multi-tenancy	V	V	V	V	V	V	V	V	-	V	V	V	V	X
Maximaal eenmalig lokale administratorrechten nodig voor het installeren van client-software	V	V	V	X	V	V	V	V	-	V	V	V	-	V
Minimaal ondersteuning voor RDP en ondersteuning voor Citrix (ICA) en VMware (PCoIP)	V	V	V	V	V	V	V	X	X	V	V	-	V	V
Bookmarks	X	V	V	V	V	V	V	V	V	V	V	-	V	V
VPN tunneling	V	V	V	V	V	V	V	V	V	V	V	V	V	V
Host-checker/EPC (End Point Control)/NAC (Network Access Control)	-	V	V	V	V	V	V	V	V	V	V	V	V	V
SNMP, Syslog en Koppeling HP ArcSight	X	V	V	V	V	V	V	V	V	V	V	V	X	X
Moet de volgende authenticatie-methode bevatten m.b.t. SSO: Kerberos, Basic & remote authenticatie en NTLM	-	V	V	V	V	V	V	V	V	V	V	V	-	V
Ondersteuning voor HTML5	-	V	V	-	V	V	V	V	-	X	V	V	V	V
Er moet een mogelijkheid zijn om alleen SSL VPN te gebruiken (webbased, clientless)	X	V	V	V	V	V	V	V	V	-	V	X	-	X

Tabel 14 Longlist uitgewerkt

3.1.7 Uitslag onderzoek longlist

Door internetbronnen te bestuderen (zoals manuals, administrator guides, technical specifications en video's van leveranciers) zijn de leveranciers allemaal beoordeeld op de gestelde '*Key Criteria*'. Per afgevallen leverancier ga ik toelichten waarom ze niet meer in aanmerking komen voor een oplossing. In tabel 14 vindt u een overzicht van alle '*Key Criteria*' per leverancier. Hierbij zijn drie mogelijkheden tot beoordelen:

V Leverancier voldoet aan de gestelde '*Key Criteria*'.
X Leverancier voldoet niet aan de gestelde '*Key Criteria*'.
- Niet van toepassing. Tijdens het onderzoek is al geconstateerd dat de leverancier niet voldoet aan een eis. Dit betekent dat de leverancier afvalt en er geen reden is voor verder onderzoek.

WatchGuard
WatchGuard is een leverancier van Network Security Appliances. De aanbieder levert onder andere: Next-Generation Firewalls, Unified Threat Management systemen, virtuele oplossingen en beveiligde wireless access points. WatchGuard biedt verschillende firewalls met opties voor SSL VPN (WatchGuard, sd).

Via de website van WatchGuard is een uitgebreide handleiding te vinden hoe SSL VPN geconfigureerd kan worden (Watchguard, 2009).

Als eerst heb ik gekeken naar de platformen die worden ondersteund. Een '*Key Criteria*' is Windows 7 en hoger, Mac OSX, iOS of Android. De enige ondersteuning die voor Android en iOS zijn gevonden, zijn IPSec opties. Dit is bijvoorbeeld te zien aan de beschrijving van de Android app in de Google Play Store. Hierin staat het volgende:

"Create fast and easy VPN connections from anywhere to WatchGuard XTM security appliances. WatchGuard Mobile VPN enables the creation of a mobile virtual private network (VPN) connection via IPSec. Your system administrator sets up the VPN at the WatchGuard firewall, exports profile settings to a file, which is then distributed via email to end users (WatchGuard Technologies Inc, 2013)*."*

WatchGuard biedt alleen de mogelijkheid om een VPN verbinding via IPSec op te zetten. Dit lijkt vreemd omdat SSL VPN gebruik maakt van een webbrowser. Echter is de portal waar als eerst wordt ingelogd alleen maar voor het downloaden van de client software om vervolgens een IPSec verbinding op te zetten.

Barracuda Networks
Barracuda Networks levert verschillende netwerk en storage oplossingen. Barracuda Networks focust zich op drie hoofdzaken, namelijk:

1) Beschermen van gegevens
2) Netwerken en application delivery
3) Data storage, bescherming en disaster recovery

Barracuda biedt een SSL VPN oplossing aan die draait op hun SSL VPN appliance. Een voorbeeld hiervan is de Barracuda SSL VPN 880 (ntsecurity.com, sd).

Op de website van Barracuda is via de zoekopdrachtenbalk al veel informatie te vinden. Echter kon ik er na het bestuderen van de website en de documenten op de website niet achter komen of er bij een update administrator rechten nodig zijn.

In mijn browser kreeg ik de optie om een chat te openen. Zoals te zien is in bijlage 2 heb ik via deze weg een antwoord op mijn vraag gekregen. Jammer genoeg blijkt dat er een grote kans is dat de oplossing van Barracuda Networks gebruikersproblemen op gaat leveren. Om deze reden is deze oplossing afgevallen.

Citrix
Citrix is een grote speler op markten als virtualisatie, cloud computing, netwerken en mobiliteit (DeBeasi, 2014). De kracht van deze onderneming ligt in de diversiteit. Zo bieden ze oplossingen aan voor virtuele desktops, netwerkoptimalisatie en beveiliging, cloud oplossingen en oplossingen voor mobiliteit.

Een eis vanuit Motiv is dat een VPN oplossing virtuele desktops van zowel Citrix als Vmware moet kunnen aanbieden. De oplossing van Citrix biedt hier echter geen mogelijkheid toe. Om deze reden valt de Netscaler van Citrix af.

Sangfor
Sangfor is een grote speler op het gebied van netwerkbeveiliging, management en optimalisatie oplossingen op de Aziatische markt. Binnen Motiv is deze leverancier onbekend. Om informatie te verzamelen over de SSL-VPN oplossing die Sangfor biedt, is er informatie verzameld op de website. Hier valt wel het een en ander te vinden, echter is er op drie '*Key Criteria*' geen antwoord gevonden. Daarom heb ik een mailbericht naar de support afdeling van Sangfor gestuurd. Op mijn eerste bericht is echter na een week nog geen antwoord gekomen. Na een week is er nog een tweede mailbericht (zie bijlage 2) naar de support afdeling van Sangfor gestuurd. Deze is echter ook onbeantwoord gebleven. Omdat een antwoord van Sangfor te lang uitblijft, wordt deze leverancier niet verder meegenomen in het onderzoek.

Cryptzone
Cryptzone beveiligt bedrijfsnetwerken met dynamische oplossingen. De focus ligt op het beschermen van kritieke services en applicaties. Gezien de nieuwe technieken verplaatst ook de focus van Cryptzone steeds meer naar de cloud. Aan de hand van internetbronnen en de eigen website van Cryptzone is er het een en ander aan informatie gevonden. Voor de overige vragen heb ik een mail gestuurd naar de support afdeling van Cryptzone (zie bijlage 2). Hierop is echter na twee weken nog geen antwoord op ontvangen. Om deze reden wordt de oplossing van Cryptzone niet verder meegenomen in het onderzoek.

Palo Alto Networks
Palo Alto Networks is een netwerk en netwerkbeveiligingsbedrijf. Het bedrijf levert netwerkapparatuur en verschillende oplossingen. Eén van hun oplossingen is 'GlobalProtect'. Dit is een oplossing die zorgt voor een veilige verbinding met het bedrijfsnetwerk.

Palo Alto Networks is afgevallen omdat zij geen webbased oplossing bieden. De werking is vergelijkbaar met de oplossing van WatchGuard. Via de webbrowser kunnen gebruikers inloggen om vervolgens software te downloaden. Daarna kan er een IPSec verbinding tot stand worden gebracht (Palo Alto Networks, 2016).

Array Networks
Array Networks levert netwerkapparatuur en -tools voor veilig netwerkverkeer. De oplossing die Array Networks biedt kan zowel virtueel als fysiek worden uitgerold.

De oplossing van Array Networks biedt geen directe koppeling met de ArcSight SIEM oplossing (HP, 2016), dit is echter wel een vereiste. Om deze reden wordt de oplossing niet verder meegenomen in het onderzoek.

NetMotion Wireless
NetMotion Wireless is een bedrijf dat zich focust op het ontwikkelen van software oplossingen. Hierbij ligt de focus op security. De VPN oplossing die NetMotion ontwikkeld heeft, heet Mobility XE.

De oplossing valt bij de eerste selectie ronde al af om een aantal redenen. Zo is de oplossing niet clientless te gebruiken en niet multi-tenant uit te voeren. Ook is er geen directe koppeling mogelijk met ArcSight. Hiervoor is maatwerk nodig.

NetBoss is de leverancier in Nederland voor het product van NetMotion. Via de telefoon en de mail is er contact geweest met Stefan van Vlerken die mijn vragen heeft beantwoord (zie bijlage 2).

3.2 Eisen en wensen van Motiv en haar klanten
Na een voorselectie van leveranciers die binnen de harde eisen vallen, is het zaak om de selectie van leveranciers verder te verkleinen. Om dit te kunnen doen is het belangrijk dat de eisen en wensen vanuit Motiv en haar klanten bekend zijn. Deze informatie wordt verkregen uit interviews en enquêtes. De eerste stap is het bedenken van de juiste vragen om zo goed mogelijk voorbereid te zijn op de interviews. Ook is er een enquête voorbereidt voor de klanten van Motiv. De voorbereiding op de interviews en enquêtes vindt u in bijlage 3. Hieronder vindt u de eisen en wensen die uit de interviews en enquêtes zijn voortgekomen.

3.2.1 Categoriseren en prioriteren van eisen en wensen
Om een duidelijk overzicht te creëren van de verschillende eisen en wensen, is er gekozen voor het maken van verschillende categorieën:

Fx* = Functionele eis/wens
Bx = Beheer eis/wens
Sx = Security eis/wens
Kx = Kosten eis/wens
Tx = Technische eis/wens
* De x staat hierbij voor volgnummer

Aan de hand van de MoSCoW methode kunnen zijn de volgende prioriteiten voor de eisen en wensen gedefinieerd:

- Must have (wegingsfactor 4)
- Should have (wegingsfactor 3)
- Could have (wegingsfactor 2)
- Would like to have (wegingsfactor 1)

De eisen en wensen die voort zijn gekomen uit interviews met de productmanager (Bart Verhaar), bedrijfsbegeleider (Simon van den Bos), de technische diensteigenaar (Fabian Gugelot) en de uitslagen van de enquêtes onder klanten zijn hieronder per categorie opgesteld.

3.2.2 Kosten

Voor de kosten zijn er uit het interview vier eisen/wensen naar voren gekomen. De eerste heeft betrekking op de aanschaf van licenties. Een concurrent user licentiemodel betekent dat er alleen licenties nodig zijn voor actieve gebruikers. Wanneer een gebruiker de sessie eindigt, kan iemand anders deze gebruiken. Dit is niet essentieel, maar moet wel worden meegenomen in de score. Vandaar de weging 2 (Could have). Omdat de vraag hierop alleen met ‘ja’ of ‘nee’ beantwoord kan worden, is er gekozen voor een score van 10 of 0.

De tweede eis die betrekking heeft op de kosten betreft een MSP (Managed Service Provider) model voor licenties. Dit betekent hoe meer er wordt aangeschaft, hoe hoger de korting zal zijn. Deze vraag kan wederom met ‘ja’ of ‘nee’ beantwoord worden. Het model is geen eis, maar is wel wenselijk. Om deze reden is er gekozen voor wegingsfactor 1.

Voor de derde eis is een case bedacht. Uit deze case moet naar voren komen welke leverancier het beste scoort op de algehele kosten. Dit is erg belangrijk en heeft een wegingsfactor van 4. De case bestaat uit de kosten voor:

- SSL VPN appliance voor minimaal vijftig concurrent users
- Drie jaar 24/7 support
- Licentiekosten

Het is de bedoeling dat per leverancier al deze kosten bij elkaar worden opgeteld. De goedkoopste oplossing scoort een 10, de duurste een 0. Alles wordt berekend zoals in het onderstaande voorbeeld:

Leverancier A: €1.000,-
Leverancier B: €600,-
Leverancier C: €750,-

Hier scoort A een 0 en B een 10. Het verschil is 400. Dat betekent per €40 een punt. Leverancier C is €150,- duurder dan leverancier B. €150/40=4 dus scoort C (10-4=) 6.

Naast de kostencase is het ook van belang dat de relatie wordt meegenomen in de score. Hiervoor is wens K4 bedacht. Er zijn leveranciers waar heel goed contact mee is en die reeds partner zijn van Motiv. Deze leveranciers scoren een 10. Wanneer er goed contact is, maar nog geen partnership, scoort deze een 5.

Nr.	Eis/wens m.b.t. de kosten	Weging	Bepalen van de score
K1	Een concurrent user licentiemodel	2	Ja = 10, nee = 0
K2	MSP model voor licenties	1	Ja = 10, nee = 0
K3	Kosten	4	Kostencase
K4	Partnership met Motiv	2	Ja=10, gedeeltelijk = 5, nee = 0

Tabel 15 Kosten eisen en wensen

3.2.3 Functies

Uit de interviews zijn functies van de oplossing naar voren gekomen. Zo is het wenselijk dat de oplossing een losse appliance is in plaats van een firewall oplossing. Dit omdat de klanten van Motiv al voorzien zijn van een firewall en deze oplossing alleen de telewerkdienst betreft. Hiervoor is een weging van 2 bepaald.

Het is wenselijk om de portal aan te passen. Zo is de portal voor de gebruikers te herkennen aan bijvoorbeeld een logo of eigen huisstijl. Het aanpassen van de portal is echter geen vereiste. Hierbij is gekozen voor een weging van 1 en een score tussen de 0 en 10 die wordt bepaald door functies als aanpassen logo, huisstijl en achtergrond.

Zoals al eerder besproken wordt er steeds vaker gebruik gemaakt van smartphones en tablets. Om deze reden is het belangrijk dat de oplossing mobiele browsers ondersteunt.

Nr.	Eis/wens m.b.t. de functies	Weging	Bepalen van de score
F1	Op zichzelf staande oplossing i.p.v. firewall	2	Ja = 10, nee = 0
F2	Aanpassen van portal, zoals logo, huisstijl en achtergrond	4	Volledig aanpasbaar = 10, gedeeltelijk = 4, niet aanpasbaar = 0
F3	Mobiele pagina voor smartphones en tablets	3	Ja = 10, nee = 0

Tabel 16 Functionele eisen en wensen

3.2.4 Beheerbaarheid

Voor het beheer van de telewerkoplossing zijn een aantal eisen en wensen opgesteld. De eerste eis is de mogelijkheid van 24/7 support. Motiv biedt deze supportoptie ook aan hun eigen klanten. Wanneer nodig moet Motiv kunnen schakelen met de leverancier. Dit is zeer belangrijk en heeft een weging van 4.

Daarbij is het handig als de klant direct contact op kan nemen met de leverancier. Deze wens heeft een weging van 2.

Motiv heeft klanten die grotendeels van hun appliances virtueel draaien. Deze zitten niet te wachten op het aanschaffen van hardware. Om deze reden is eis B3 opgesteld met een weging van 3.

Nr.	Eis/wens m.b.t. de beheerbaarheid	Weging	Bepalen van de score
B1	Support: 24/7 bereikbaar	4	Ja = 10, nee = 0
B2	Directe support voor de klant met de leverancier	2	Ja = 10, nee = 0
B3	De oplossing kan virtueel draaien	3	Ja = 10, nee = 0

Tabel 17 Beheer eisen en wensen

3.2.5 Security

Logischerwijs heeft Motiv de beveiliging van systemen hoog in het vaandel staan. Onderstaande eisen zijn opgesteld om ervoor te zorgen dat het bedrijfsnetwerk veilig toegankelijk is en ter bescherming van bedrijfsgevoelige data.

De host-check zorgt voor een controle op een endpoint. Voor de host-check wil Motiv minimaal de volgende gegevens kunnen controleren: antivirus, updates, laatste virusscan, processen en of het apparaat lid is van het domein. Aan de hand van deze host-check worden de resources bepaald waar een gebruiker toegang toe heeft. De host-check is een eis en scoort op de verschillende gegevens zoals hierboven genoemd.

Om verdacht verkeer op te sporen en te blokkeren dient de SSL VPN oplossing gekoppeld te kunnen worden met een Intrusion Prevention System (IPS) en een Intrusion Detection System (IDS). Dit is wenselijk en heeft een weging van 2. Omdat de weging 2 is, wordt dit alleen onderzocht en dus niet meegenomen naar de testfase.

Wanneer een SSL VPN verbinding wordt beëindigd, dienen er geen gegevens meer achter te blijven op de client en de server. Gegevens zoals cache, cookies en opgeslagen wachtwoorden dienen gewist te worden. De SSL VPN appliance dient dit te forceren.

Een belangrijke eis is Role based access control als mogelijkheid. Dit betekent dat er per groep of gebruiker verschillende rechten ingesteld kunnen worden. Denk hierbij aan rechten voor toegang tot bepaalde shares en het uitdelen van rechten voor beheer.

De laatste security eis betreft de verschillende rollen per authenticatiemethode. Het moet mogelijk zijn om gebruikers die op een minder beveiligde manier inloggen (bijvoorbeeld zonder two-factor authentication) beperkte toegang te kunnen geven.

Nr.	Eis/wens m.b.t. de functies	Weging	Bepalen van de score
S1	Host-check: antivirus, updates, lid van domain, register, laatste virus scan, processen	3	antivirus = 2, updates = 2, lid van domain = 2, register = 1, laatste scan = 2, processen = 1
S2	Koppeling met Intrusion Prevention System	2	full = 10, gedeeltelijk = 5, niet = 0
S3	Koppeling met Intrusion Detection System	2	full = 10, gedeeltelijk = 5, niet = 0
S4	Hostcheck vóór authenticatie en na authenticatie	2	voor authenticatie = 7, na authenticatie = 3
S5	Cache, cookies en opgeslagen wachtwoorden verwijderen op de client	4	cache = 3, cookies = 3, opgeslagen wachtwoorden = 4
S6	Cache, cookies en opgeslagen wachtwoorden verwijderen op de server	4	cache = 3, cookies = 3, opgeslagen wachtwoorden = 4
S7	Role based access control	4	ja = 10, nee = 0
S8	Verschillende rollen per authenticatiemethode	4	ja = 10, nee = 0

Tabel 18 Security eisen en wensen

3.2.6 Techniek

De technische eisen en wensen zijn opgesomd in tabel 19.

De eerste eis is dat de oplossing een mogelijkheid moet hebben om via verschillende URL's benaderd te worden. Per URL dient er een ander certificaat afgegeven te worden.

Een managementoverzicht van alle te beheren domeinen is wenselijk. Om deze reden heeft T2 een weging van 1.

De klanten van Motiv die de enquête (bijlage 4) hebben ingevuld, vinden het belangrijk dat er snel ondersteuning is voor nieuwe OS'en. Hiervoor is wederom een case bedacht die per leverancier zal bepalen welke het snelste een update aanbiedt voor een nieuw OS. Hierbij wordt de scoren 0 t/m 10 gegeven, waarbij 10 voor de snelste aanbieder en 0 voor de langzaamste aanbieder.

De overige eisen en wensen spreken voor zich en zijn te vinden in onderstaande tabel.

Nr.	Eis/wens m.b.t. de functies	Weging	Bepalen van de score
T1	Meerdere URL's met eigen certificaat	3	meerdere URL's = 5, certificaat per URL = 5
T2	Management: overzicht alle domeinen	1	ja = 10, nee = 0
T3	Ondersteuning voor nieuwe OS'en	2	Per leverancier tijd bepalen, snelste =10 afhankelijk van de tijd die er tussen zit wordt de score bepaald
T4	VLAN ondersteuning	1	ja = 10, nee = 0
T5	Failover: active/active	2	ja = 10, nee = 0
T6	Failover: active/passive	4	ja = 10, nee = 0
T7	IPV6 ondersteuning	4	ja = 10, nee = 0
T8	Back-up: config, users en licenties	4	config = 4, users = 3, licenties =3
T9	Schaalbaarheid: loadbalancing	3	goede mogelijkheden voor loadbalancing = 10, gematigde mogelijkheden = 6, niet = 0

Tabel 19 Technische eisen en wensen

3.3 Uitslag shortlist

Per onderwerp is een tabel gemaakt voor de scores. In dezelfde tabel vindt u de weging per eis of wens en de leveranciers. Is de eerste kolom staat de score per leverancier, in de tweede kolom de score maal de weging.

Eisen/wensen m.b.t. de kosten													
Nr.	Weging	F5 Networks (score)	F5 Networks (score x weging)	Cisco (score)	Cisco (score x weging)	Pulse (score)	Pulse (score x weging)	Fortinet (score)	Fortinet (score x weging)	Dell (score)	Dell (score x weging)	Check Point (score)	Check Point (score x weging)
K1	2	10	20	10	20	10	20	0	0	10	20	10	20
K2	1	10	10	0	0	10	10	10	10		0	0	0
K3	4	3	12	7	28	0	0	10	40		0	8	32
K4	2	10	20	5	10	10	20	5	10	0	0	10	20
Totaal		**33**	**62**	**22**	**58**	**30**	**50**	**25**	**60**	**10**	**20**	**28**	**72**

Tabel 20 Eisen/wensen m.b.t. de kosten

In de eerste tabel vindt u de kosten van de eisen en wensen. Eén grote afwijking valt direct op: K2 en K3 zijn voor Dell niet ingevuld. Deze eis en wens zijn open gebleven en niet te achterhalen vanuit Motiv, omdat er geen sprake is van een partnership. Om te kijken of dit niet van te grote invloed is, heb ik in beide vakken een 10 genoteerd. Echter Komt Dell dan nog niet in aanmerking voor het *proof of concept*. Om de vergelijking eerlijk weer te geven heb ik vervolgens de score open gelaten.

De tweede afwijking is te zien bij wens K4. Dit heeft betrekking op het partnership met Motiv. Cisco en Fortinet scoren hier een 5. Dit wijkt af van de standaard 10 (wanneer het antwoord 'ja' is) of 0 (wanneer het antwoord 'nee' is). Cisco is namelijk wel een partner van Motiv, maar volgens Bart Verhaar (Productmanager Motiv) is het contact met Cisco minder goed dan met andere leveranciers. Samen brengt dit een score van 5.

Fortinet is geen partner van Motiv. Echter is er wel sprake van goed contact. Dit zorgt ervoor dat Fortinet hier ook 5 punten scoort.

Bij eis K3 ziet u allerlei verschillende scores. Dit heeft te maken met een kostencase die is opgesteld. De vraag was: '*welke leverancier brengt de minste kosten in rekening voor een opstelling met vijftig concurrent users (licenties), drie jaar support en de benodigde hardware?*' . Uit onderzoek naar deze vraag per leverancier is onderstaande tabel voortgekomen. De gegevens zijn verzameld aan de hand van offerteaanvragen door de afdeling Sales bij Motiv. Hierbij is nadrukkelijk gevraagd naar de listprijs. Dit betekent dat er geen rekening wordt gehouden met eventuele kortingen.

Appliance	Pulse	Cisco	F5	Fortinet	Dell	Check Point
Licenties	€ 3.000,00	€ 3.595,00	€ 3.145,00	€ 473,00		€ 595,00
Support 3 jaar	€ 8.795,00	€ 100,00	€ 3.145,00	€ -		€ 1.540,00
Totaal	€ 2.920,00	€ -	€ 3.208,00	€ 312,00		€ 831,00
	€ 14.715,00	€ 3.695,00	€ 9.498,00	€ 785,00		€ 2.966,00

Tabel 21 Kostencase

Zoals al eerder gezegd is het vanuit Motiv niet mogelijk om deze gegevens voor Dell te verzamelen. De goedkoopste oplossing scoort 10 punten op de eis (Fortinet) en de duurste 0. Alles wat daar tussen zit is als volgt berekend:

Het verschil tussen de duurste oplossing en de goedkoopste oplossing bedraagt €14.000,-. Hierbij zijn 10 punten te scoren. Dat betekent (14.000/10=)1.400 per punt.

Eisen/wensen m.b.t. de functies													
Nr.	Weging	F5 Networks (score)	F5 Networks (score x weging)	Cisco (score)	Cisco (score x weging)	Pulse (score)	Pulse (score x weging)	Fortinet (score)	Fortinet (score x weging)	Dell (score)	Dell (score x weging)	Check Point (score)	Check Point (score x weging)
F1	2	0	0	0	0	10	20	0	0	0	0	0	0
F2	4	10	40	10	40	10	40	10	40	4	16	10	40
F3	3	10	30	0	0	10	30	10	30	0	0	10	30
Totaal		**20**	**70**	**10**	**40**	**30**	**90**	**20**	**70**	**4**	**16**	**20**	**70**

Tabel 22 Score functionele eisen en wensen

In tabel 22 vindt u een overzicht van de scores op de functionele eisen en wensen. Alle scores zijn 0 of 10 met uitzondering van de eis F2 bij Dell. Dit komt omdat bij de Sonicwall van Dell de portal gedeeltelijk is aan te passen. Zo kan er alleen gekozen worden voor standaard kleuren en bevat het logo een grootte die niet aan te passen is. Dit is ten opzichte van de andere oplossingen een beperking. Om deze reden scoort Dell hier 4 punten.

Eisen/wensen m.b.t. de beheerbaarheid													
Nr.	Weging	F5 Networks (score)	F5 Networks (score x weging)	Cisco (score)	Cisco (score x weging)	Pulse (score)	Pulse (score x weging)	Fortinet (score)	Fortinet (score x weging)	Dell (score)	Dell (score x weging)	Check Point (score)	Check Point (score x weging)
B1	4	10	40	10	40	10	40	10	40	10	40	10	40
B2	2	10	20	10	20	10	20	10	20	0	0	10	20
B3	3	10	30	10	30	10	30	10	30	10	30	10	30
Totaal		**30**	**90**	**30**	**90**	**30**	**90**	**30**	**90**	**20**	**70**	**30**	**90**

Tabel 23 Score beheer eisen en wensen

Bij de eisen en wensen die betrekking hebben op de beheerbaarheid zijn geen afwijkingen te vinden. Wat opvalt, is dat er slechts één keer een 0 wordt gescoord. Dell biedt namelijk geen directe support voor klanten.

Eisen/wensen m.b.t. de security													
Nr.	Weging	F5 Networks (score)	F5 Networks (score x weging)	Cisco (score)	Cisco (score x weging)	Pulse (score)	Pulse (score x weging)	Fortinet (score)	Fortinet (score x weging)	Dell (score)	Dell (score x weging)	Check Point (score)	Check Point (score x weging)
S1	3	8	24	8	24	10	30	8	24	5	15	9	27
S2	2	10	20	10	20	10	20	10	20	10	20	10	20
S3	2	10	20	10	20	10	20	10	20	10	20	10	20
S4	2	10	20	10	20	10	20	0	0	0	0	0	0
S5	4	7	28	10	40	10	40	10	40	10	40	3	12
S6	4	10	40	10	40	10	40	10	40	10	40	10	40
S7	4	10	40	10	40	10	40	10	40	0	0	10	40
Totaal		**65**	**192**	**68**	**204**	**70**	**210**	**58**	**184**	**45**	**135**	**52**	**159**

Tabel 24 Score security eisen en wensen

In tabel 24 treft u de eisen en wensen met betrekking op security. De eerste eis (S1) heeft betrekking op de hostcheck. Hier variëren de scores omdat binnen deze eis om meerdere criteria is getoetst. De hostcheck scoort op de volgende onderwerpen:

- Is het mogelijk om te controleren of de virusscanner actief is?
- Is het mogelijk om te controleren of de laatste updates geïnstalleerd zijn?
- Is het mogelijk om te controleren of de client lid is van het domein?
- Is het mogelijk om registerwaarden te controleren?
- Is het mogelijk om te controleren wanneer de laatste virusscan is uitgevoerd?
- Is het mogelijk om te controleren welke processen er actief zijn?

In onderstaande tabel ziet u hoe elke leverancier op elk punt scoort. Tussen haakjes vindt u de toe te kennen score die hierbij hoort. Door de scores per leverancier op te tellen, is de score in tabel 24 bij eis S1 tot stand gekomen.

Leveranciers/ Hostcheck	Antivirus (2)	Updates (2)	Lid van domein (2)	Register check (1)	Laatste virus scan (2)	Processen (1)
F5	V	V	X	V	V	V
Cisco	V	V	V	V	X	V
Pulse	V	V	V	V	V	V
Fortinet	V	V	V	V	X	V
Dell	V	X	V	V	X	X
Check Point	V	V	V	V	V	X

Tabel 25 Hostcheck scoren

De volgende afwijkende score is te vinden bij eis S5. F5 scoort hier een 7, omdat er geen mogelijkheid is tot het verwijderen van cookies op de client. Check Point scoort een 3, omdat er alleen maar een mogelijkheid is om cache te verwijderen van de client.

Eisen/wensen m.b.t. de techniek													
Nr.	Weging	F5 Networks (score)	F5 Networks (score x weging)	Cisco (score)	Cisco (score x weging)	Pulse (score)	Pulse (score x weging)	Fortinet (score)	Fortinet (score x weging)	Dell (score)	Dell (score x weging)	Check Point (score)	Check Point (score x weging)
T1	1	10	10	10	10	10	10	10	10	10	10	10	10
T2	4	10	40	10	40	0	0	3	12	6	24	9	36
T3	3	10	30	10	30	10	30	10	30	10	30	10	30
T4	2	10	20	10	20	10	20	10	20	10	20	10	20
T5	4	10	40	10	40	10	40	10	40	10	40	10	40
T6	4	10	40	10	40	10	40	10	40	10	40	10	40
T7	4	10	40	7	28	10	40	4	16	10	40	4	16
T8	3	10	30	10	30	10	30	10	30	10	30	10	30
Totaal		**80**	**250**	**77**	**238**	**70**	**210**	**67**	**198**	**76**	**234**	**73**	**222**

Tabel 26 Score technische eisen en wensen

Bij de technische eisen en wensen zien we de eerste afwijkende score bij T2. Voor T2 is wederom een case opgesteld. Bij T2 heb ik een score toegekend per leverancier om te kijken hoe snel zij een nieuw OS ondersteunen. Hiervoor is onderzoek gedaan naar de ondersteuning voor Windows 10. Per leverancier is gezocht naar een release datum. De verdeling van de score is vergelijkbaar met de kostencase. De weging bij T2 is aangepast (van 2 naar 4) naar aanleiding van de enquêtes. Hieruit is gebleken dat klanten van Motiv het ondersteunen van een nieuw OS belangrijker vinden dan vooraf gedacht. De uitslagen van de enquêtes vindt u in bijlage 4.

	Pulse	Cisco	F5	Fortinet	Dell	Check Point
Windows 10	16-02-16	22-05-15	14-05-15	09-12-15	02-09-15	16-06-15
rank	6	2	1	5	4	3
punten	0	10	10	3	6	9

Tabel 27 Screenshot uitslag OS Case

In tabel 27 is te zien dat F5 als eerste ondersteuning voor Windows 10 aanbood. Om deze reden scoort F5 een 10. Pulse is de laatste die ondersteuning aanbood voor Windows 10 en scoort om deze reden 0 punten. Het verschil tussen F5 en Pulse is negen maanden. Dit betekent dat een punt gelijk is aan 1,1 maand.

De volgende afwijkende scoren zijn te vinden bij T7. Deze eis bevat de mogelijkheid tot het back-uppen. Deze eis is opgedeeld in drie punten, namelijk: back-uppen van gebruikers (3 punten), back-uppen van de configuratie (4 punten) en het back-uppen van de licenties (3 punten).

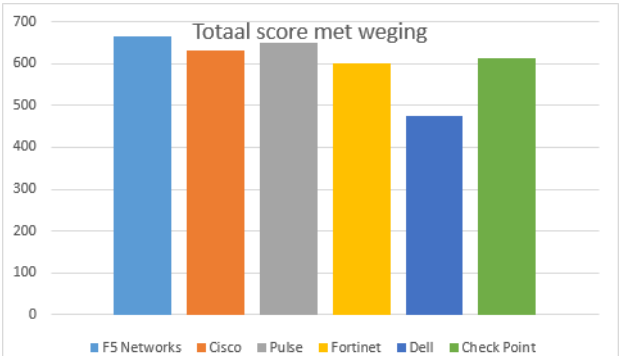
Cisco scoort hier 7 punten, omdat het back-uppen van gebruikers ontbreekt. Bij Fortinet en Check Point wordt er alleen maar gesproken over het back-uppen van de configuratie.

Als we alle eisen en wensen samen nemen en de scoren (maal weging) bij elkaar optellen, komen we tot een uitslag zoals in tabel 28.

Eisen/wensen totaaloverzicht												
Type	F5 Networks (score)	F5 Networks (score x weging)	Cisco (score)	Cisco (score x weging)	Pulse (score)	Pulse (score x weging)	Fortinet (score)	Fortinet (score x weging)	Dell (score)	Dell (score x weging)	Check Point (score)	Check Point (score x weging)
Kosten	33	**62**	22	**58**	30	**50**	25	**60**	10	**20**	28	**72**
Functies	20	**70**	10	**40**	30	**90**	20	**70**	4	**16**	20	**70**
Beheerbaarheid	30	**90**	30	**90**	30	**90**	30	**90**	20	**70**	30	**90**
Security	65	**192**	68	**204**	70	**210**	58	**184**	45	**135**	52	**159**
Techniek	80	**250**	77	**238**	70	**210**	67	**198**	76	**234**	73	**222**
Totaal	**228**	**664**	**207**	**630**	**230**	**650**	**200**	**602**	**155**	**475**	**203**	**613**

Tabel 28 Totaalscore shortlist

Om de uitslag duidelijker weer te geven is er een grafiek gemaakt waar de totale score maal de weging bij elkaar is opgeteld per leverancier. We kunnen uit deze uitslag concluderen dat Dell een duidelijke afvaller is. De rest van de leveranciers liggen dichter bij elkaar. Pulse scoort het beste, gevolgd door F5 en Cisco. Deze drie leveranciers zullen worden meegenomen naar de volgende fasen. Er zullen drie testopstellingen worden gerealiseerd.



Figuur 6 Grafiek uitslag shortlist

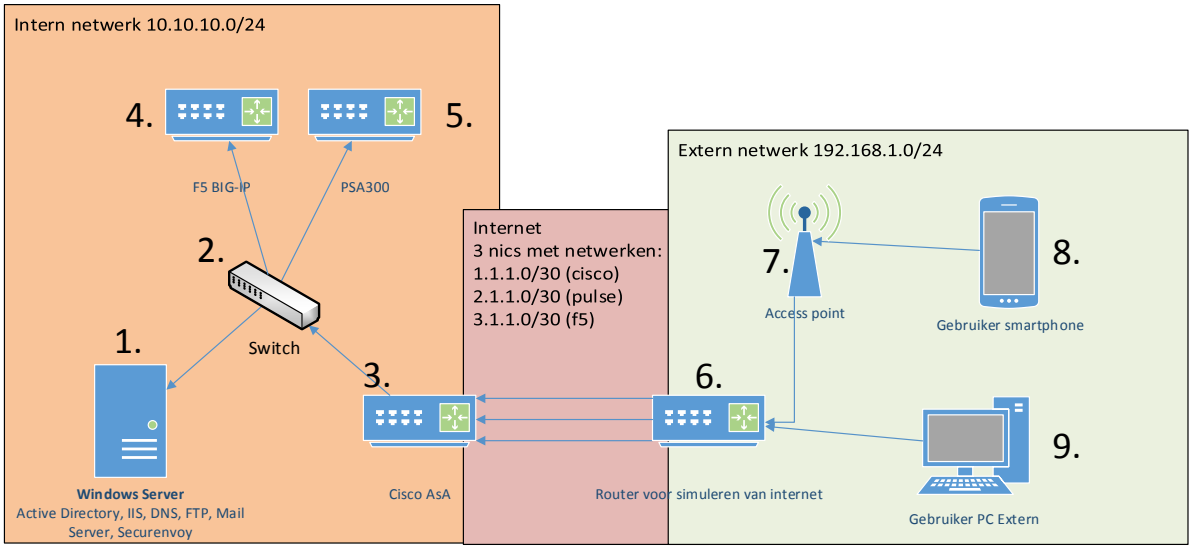
3.4 Proof of concept

Om uiteindelijke de best scorende oplossingen te kunnen testen in een testopstelling, moet deze eerst worden gebouwd in het lab van Motiv. Deze testopstelling mag alleen gebouwd worden wanneer er een duidelijke tekening is gemaakt van de opstelling. Deze moet goedgekeurd worden door Alex Maasdam (Security Engineer op de afdeling Professional Services bij Motiv). In dit hoofdstuk wordt per testopstelling een tekening opgesteld inclusief de bijbehorende configuratie. Hierbij wordt al rekening gehouden met de te testen onderwerpen.

Er worden drie verschillende testomgevingen gebouwd. Een voor het testen van Pulse Secure, een voor het testen van F5 BIG-IP en een met de Cisco ASA.

3.4.1 Pulse Secure en F5 Networks lab opstelling

In onderstaande figuur (figuur 7) vindt u de testopstelling voor de oplossing van Pulse Secure en F5 Networks. Hierbij worden drie netwerken gerealiseerd. Het interne netwerk kan worden gezien als bedrijfsnetwerk. Het externe netwerk kunt u zien als een thuisnetwerk. Daartussen wordt het internet gesimuleerd. Dit is een apart netwerk tussen het interne en externe netwerk in. Er is dus geen sprake van een echte internetverbinding.



Figuur 7 Pulse Secure en F5 Networks lab opstelling

In figuur 7 ziet u per apparaat een nummer. Per nummer worden hieronder de gegevens beschreven van bijvoorbeeld systeemvereisten, services en IP-adressen.

1. Windows Server 2012 R2
Is een Windows server 2012 R2 systeem met de volgende services:
- Active directory
- IIS Webserver
- FTP
- DNS
- Mail
- SecurEnvoy

Systeemvereisten:
- 2GHz (64-bit processor)
- 8 GB RAM
- 60 GB HDD

2. Switch
Nodig voor connectiviteit van het interne netwerk.

3. Cisco ASA
Dient als firewall voor internet netwerk. Van buitenaf moet er toegang worden toegestaan op poort 443. Dit is nodig om van buiten de SSL VPN portal te benaderen. Wanneer een externe gebruiker via de webbrowser naar https://1.1.1.1 gaat, moet de connectie worden toegestaan op 10.10.10.100:443.

Op de Cisco ASA worden 2 interfaces geconfigureerd. Op de interface in het interne netwerk wordt IP-adres 10.10.10.1/24 geconfigureerd. Op de interface naar het internet is dat 1.1.1.1/30.

4. F5 BIG-IP
Hier komt de SSL VPN Appliance van F5 Networks. Voor de F5 Networks opstelling wordt de BIG-IP (virtual edition) gebruikt. In beide gevallen krijgt het apparaat het interne IP-adres 10.10.10.100/24. De default gateway is 10.10.10.1.

5. PSA300
Voor het testen van de Pulse Secure oplossing, wordt gebruik gemaakt van een virtuele appliance.

6. Router
De router dient als gateway voor het externe netwerk. De interface van het externe netwerk krijgt het IP-adres 192.168.1.1/24. De interface naar het internet krijgt 1.1.1.2/30. Daarnaast wordt een loopback geconfigureerd op 2.2.2.2/32 om het internet te simuleren. DHCP wordt geconfigureerd voor het externe netwerk.

7. Wireless Access Point
Om een SSL VPN verbinding te kunnen testen vanaf een smartphone of tablet is er een Wireless Access Point nodig. De access point krijgt een IP-adres van de router, evenals de devices die hier een verbinding mee maken.

8. Gebruiker smartphone
Voor het testen van de mogelijkheden met iOS en Android. Zelf ben ik in bezit van beide typen toestellen en ik zal deze dus zelf meenemen voor de test.

9. Gebruiker PC Extern

Windows 7 client pc die deel uitmaakt van het externe netwerk. Krijgt een IP-adres van de router (DHCP). Minimale systeemvereisten voor de client pc zijn:

- 2GHz (64-bit processor)
- 4 GB RAM
- 30 GB HDD

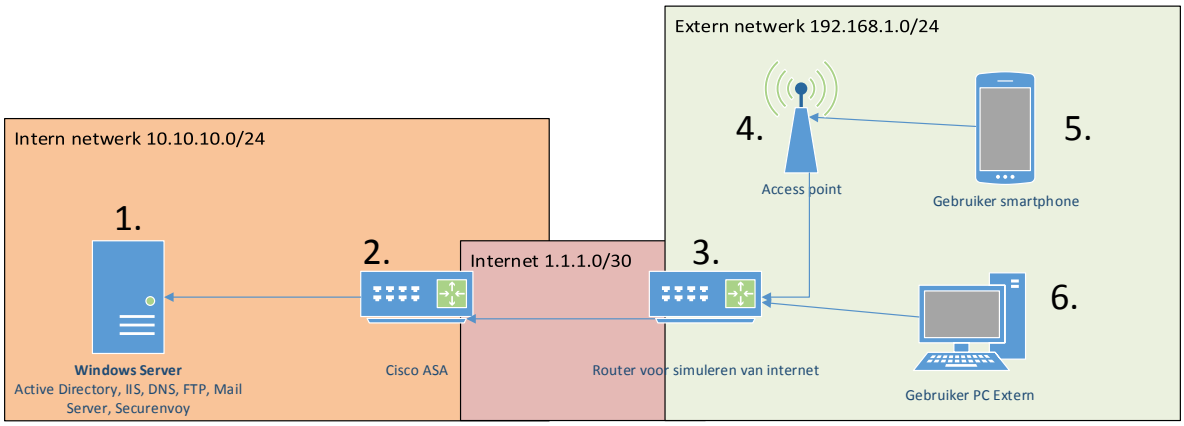
Device ID	Naam	Interface/netwerk	IP adres	Default gateway
1	Windows Server	Intern	10.10.10.10/24	10.10.10.1/24
3	Cisco ASA	Intern	10.10.10.1/24	
4	PSA300/F5 BIG-IP	Intern	10.10.10.100/24	10.10.10.1/24
3	Cisco ASA	Internet	1.1.1.1/30	
5	Router	Internet	1.1.1.2/30	
5	Router	Extern	192.168.1.1/24	
5	Router	Loopback	2.2.2.2/32	
6	Access point	Extern	DHCP*	192.168.1.1/24
7	Smartphone	Extern	DHCP*	192.168.1.1/24
8	PC extern	Extern	DHCP*	192.168.1.1/24

Tabel 29 IP-tabel Pulse Secure lab opstelling

* DHCP wordt geconfigureerd op de router (nummer 5) en bevat een range van 192.168.1.50-192.168.1.100.

3.4.2 Cisco ASA lab opstelling

De testomgeving voor de Cisco ASA SSL VPN zal iets minder complex zijn. Dit omdat de SSL VPN optie in de firewall zit. De bijbehorende tekening ziet er dan als volgt uit:



Figuur 8 Cisco lab opstelling

1. Windows Server 2012 R2/

Een Windows server 2012 R2 is een systeem met de volgende services:

- Active directory
- IIS Webserver
- FTP
- DNS
- Mail
- SecurEnvoy

Systeemvereisten:

- 2GHz (64-bit processor)

- 8 GB RAM
- 60 GB HDD

2. Cisco ASA
Cisco ASA dient als firewall voor het interne netwerk en biedt de functionaliteit voor het maken van een SSL VPN verbinding.

Van buitenaf moet er toegang worden toegestaan op poort 443. Dit is nodig om van buiten de SSL VPN portal te benaderen. Wanneer een externe gebruiker via de webbrowser naar https://1.1.1.1 gaat, wordt er toegang gevraagd op 1.1.1.1:443.

Op de Cisco ASA worden twee interfaces geconfigureerd. Op de interface in het interne netwerk wordt IP-adres 10.10.10.1/24 geconfigureerd, op de interface naar het internet 1.1.1.1/30.

3. Router
De router dient als gateway voor het externe netwerk. De interface van het externe netwerk krijgt het IP-adres 192.168.1.1/24, de interface naar het internet 1.1.1.2/30. Daarnaast wordt er een loopback geconfigureerd met het adres 2.2.2.2/32 om het internet te simuleren. DHCP wordt geconfigureerd voor het externe netwerk.

4. Wireless Access Point
Om een SSL VPN verbinding te kunnen testen vanaf een smartphone of tablet is er een Wireless Access Point nodig. De access point krijgt een IP-adres van de router, evenals de devices die hier een verbinding mee maken.

5. Gebruiker smartphone
Voor het testen van de mogelijkheden met iOS en Android. Zelf ben ik in bezit van beide typen toestellen en zal deze dus zelf meenemen voor de test.

6. Gebruiker PC Extern
Windows 7 client pc die deel uitmaakt van het externe netwerk. Krijgt een IP-adres van de router (DHCP). Minimale systeemvereisten voor de client pc zijn:
- 2GHz (64-bit processor)
- 4 GB RAM
- 30 GB HDD

Device ID	Naam	Interface/netwerk	IP adres	Default gateway
1	Windows Server	Intern	10.10.10.10/24	10.10.10.1/24
2	Cisco ASA	Intern	10.10.10.1/24	
2	Cisco ASA	Internet	1.1.1.1/30	
3	Router	Internet	1.1.1.2/30	
3	Router	Extern	192.168.1.1/24	
3	Router	Loopback	2.2.2.2/32	
4	Access point	Extern	DHCP*	192.168.1.1/24
5	Smartphone	Extern	DHCP*	192.168.1.1/24
6	PC extern	Extern	DHCP*	192.168.1.1/24

Tabel 30 IP Tabel Cisco ASA

** DHCP wordt geconfigureerd op de router (nummer 3) en bevat een range van 192.168.1.50-192.168.1.100.*

3.5 Testresultaten

Voor het testen van de verschillende opstellingen is vooraf een testplan template opgesteld waarin de belangrijkste eisen en wensen naar voren komen. De testplan template is te vinden in bijlage 6 van dit document. Bij het opstellen van het testplan is rekening gehouden met de eisen en wensen vanuit Motiv, maar ook vanuit de klant. Zo wil de klant graag met twee monitoren kunnen werken op de nieuwste besturingssystemen. Voor de twee monitoren is een test toegevoegd. Alle gebruikerstesten worden uitgevoerd op een Windows 10 machine.

Deze template is ingevuld voor alle drie de leveranciers. De resultaten per leverancier vindt u in bijlage 7.

Verder in dit hoofdstuk zal ik per leverancier de testresultaten samenvatten.

Cisco ASA

De Cisco ASA scoorde matig in de test. Dit komt mede door het niet kunnen testen van alle functionaliteiten. Er zijn licenties nodig waarmee plug-ins gedownload kunnen worden. Deze licentie is voor Motiv niet gemakkelijk te verkrijgen. Omdat er erg veel tijd heeft gezeten in het verkrijgen van een licentie (die uiteindelijk niet is verkregen), is er gekozen om te testen zonder plug-ins. Onderdelen die niet getest konden worden, hebben alsnog gescoord aan de hand van een bronnenonderzoek.

Cisco heeft het laagst gescoord omdat zij achterblijven op de Cachecleaner test en de gebruikerstesten. Zo is het niet mogelijk om cache en cookies van een server te verwijderen na een sessie. Ook is het niet mogelijk om met meerdere monitoren te werken. Hier hechten klanten van Motiv echter wel veel waarde aan.

Een compleet overzicht van de test inclusief screenshots vindt u in bijlage 7.

F5 Big-IP APM

De F5 Big-IP APM eindigt op de tweede plaats. De APM (Access Policy Manager) biedt eenvoudige opties voor het configureren van verschillende rules. De F5 Big-IP APM biedt vele mogelijkheden voor de hostscan.

F5 blijft momenteel nog achter op de Cachecleaner. Na een sessie zijn er geen mogelijkheden om de cache en cookies van een server te verwijderen. Ook scoort F5 niet de volle punten op rolebased access control en rollen per authenticatiemethode. Dit komt omdat het configureren hiervan vrij complex is. Ook het achterhalen van deze hiërarchie is lastig.

De volledige punten op de twee RDP testen blijven ook uit. De mogelijkheden tot het starten van een RDP sessie beperken zich tot HTML5.

Een compleet overzicht van de test inclusief screenshots vindt u in bijlage 7.

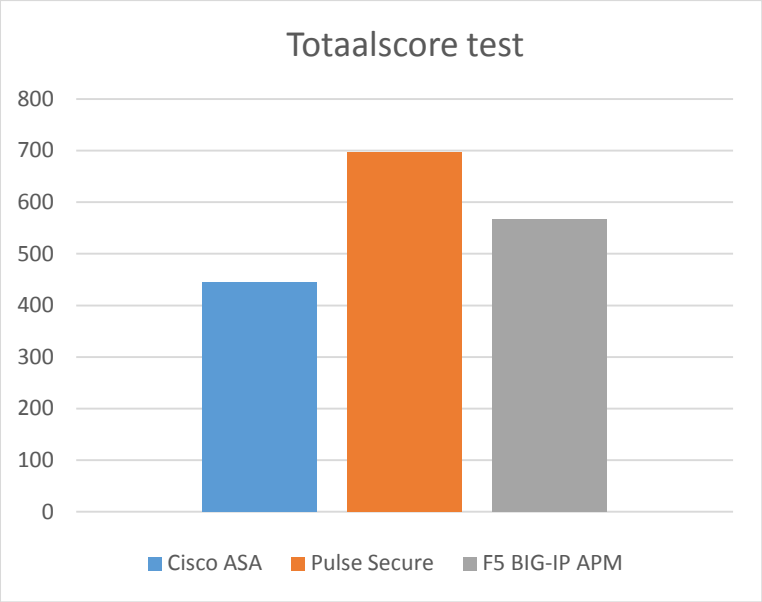
Pulse Secure

Pulse Secure komt als beste uit de test. Deze SSL VPN-oplossing scoort op bijna alles, behalve het werken met twee monitoren. Dit heb ik niet goed kunnen testen omdat er in de virtuele omgeving niet met dubbele schermen gewerkt kan worden. Zelf was ik nog niet bekend met de Pulse Secure appliance. Echter spreekt het product voor zich en is deze eenvoudig te configureren. In tabel 31 is een overzicht te zien waar er aan alle drie de leveranciers punten zijn toegekend per test. Onderaan de tabel vindt u de totaalscore. In bijlage 7 vindt u een gedetailleerd overzicht van de uitgevoerde testen.

Test	Cisco ASA	Pulse Secure	F5 Big-IP APM
H1	0	18	30
H2	18	24	30
H3	24	30	30
H4	30	30	30
H5	30	30	30
H6	0	30	15
C1	32	40	40
C2	32	40	40
C3	32	40	40
C4	0	40	0
C5	0	32	0
T1	40	40	40
T2	40	40	40
T3	40	40	28
T4	40	40	28
G1	15	30	30
G2	0	0	0
G3	20	40	24
G4	0	40	20
G5	32	32	32
G6	20	40	40
Totaal	**445**	**696**	**567**

Tabel 31 Totaalscore na testen

De totale scoren uit de verschillende testen zijn te vinden in tabel 31. Per test is een score van 0 ten en met 10 gegeven. Deze is vermenigvuldigd met de weging die bij de test hoort. De totale score per oplossing is een optelsom van alle uitgevoerde testen. De totaalscore is grafisch weergegeven in figuur 9.



Figuur 9 Grafische weergave totaalscore test

3.6 Conclusie

Tijdens de afstudeerperiode is er onderzoek gedaan naar welke SSL-VPN oplossing het best aansluit bij de huidige eisen en wensen van Motiv en haar klanten. De hoofdvraag bij dit onderzoek luidt als volgt: *"Welke SSL-VPN oplossing past het beste bij de huidige eisen en wensen van Motiv en haar klanten?"*

Na het maken van een productselectie, bestaande uit een longlist en shortlist, is er een *proof of concept* gebouwd. Op de drie overgebleven oplossingen zijn verschillende testen uitgevoerd. De uitslagen van de testen resulteren in een antwoord op de eerder genoemde hoofdvraag. We kunnen concluderen dat de oplossing van Pulse Secure het meest past bij de huidige eisen en wensen van Motiv en haar klanten.

Pulse Secure blijkt het meest complete pakket bevonden als we kijken naar de eisen en wensen van Motiv en haar klanten. De configuratie van Pulse Secure heeft grote voordelen. Bovendien is de toepassing voor iemand die het product niet kent en enige verstand van techniek heeft, eenvoudig te configureren.

De verschillen in de scoren zijn voornamelijk tot stand gekomen omdat de oplossing van Pulse Secure beter scoort op de Cache Cleaner en meerder opties biedt met betrekking tot remote desktop. Ook de eenvoud van rolebased access control en verschillende rechten per authenticatiemethode spelen een belangrijke rol. Het product is erg overzichtelijk voor de beheerder en het makkelijkst te gebruiken door de gebruikers. Gebruikers hebben geen administrator-rechten nodig om de client software te installeren. Dit voorkomt een hoop gebruikersproblemen.

3.7 Advies aan Motiv

Mijn advies aan Motiv is om de oplossing van Pulse Secure te gebruiken en aan te bieden zoals dat op dit moment al gedaan wordt. Wel adviseer ik om meer informatie te verstrekken over wat de oplossing zo uniek maakt. Momenteel wordt er op de website van Motiv vooral gesproken over de veiligheid van de oplossing. Dit is zeker het belangrijkste aspect, aangezien de dienst 'Veilig Telewerken' heet. Echter is het tevens van belang om over het beheers- en gebruikersgemak ten opzichte van andere oplossingen te vertellen. Met name grotere organisaties kunnen hier veel tijd besparen, omdat er met deze oplossing minder gebruikersproblemen voor zullen komen.

Accountmanagers kunnen, met de wetenschap dat Pulse Secure na tien jaar nog steeds het beste aansluit bij de eisen en wensen van Motiv en haar klanten, meer aansturen op het afnemen van de dienst 'Veilig Telewerken' bij de klanten.

4.0 Overzicht bronvermeldingen, figuren, tabellen en bijlages

4.1 Bronvermeldingen

An overview of the SSL or TLS handshake. (2014). Retrieved from ibm.com: http://www-01.ibm.com/support/knowledgecenter/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm?lang=en

Artikel 6 Stageovereenkomst. (2016, Februari). *Stageovereenkomst*. IJsselstein: Motiv ICT Security.

ASL BiSL Foundation. (2006, februari 1). *Downloads.* Retrieved from ASLBiSLFoundation.org.nl: http://aslbislfoundation.org/nl/

Bastiaan Bakker, P. S. (2014, Mei 20). *Fabrikanten documenten.* Retrieved from Motown: https://motown.motiv.nl/Site/Fabrikanten/Documenten%20met%20accreditatie/DC%20Cloud%20en%20datacenter%20security%20diensten%201.2.pdf

bestuurszaken.be. (n.d.). *Definitie telewerk*. Retrieved from bestuurzaken.be: https://www.bestuurszaken.be/definitie-telewerk

Crawford, J. T. (2011, April 14). *How VPNs Work*. Retrieved from Howstuffworks: http://computer.howstuffworks.com/vpn.htm

DeBeasi, P. (2014, december 22). *Vendor Rating: Citrix.* Retrieved from Gartner: http://www.gartner.com/document/2949722?ref=solrAll&refval=164021515&qid=6187faaf3baba1d3b3713c6d8d916a63

Eveleens, W. (2006). *Rendement en risico's van telewerken.* Den Haag: Sdu Uitgevers.

Fabian Gugelot, S. v. (2016, februari 24). Eisen en wensen voor een SSL VPN oplossing. (W. v. Zalm, Interviewer)

Faura, X. G. (2005). *Understanding VPN tunnels over SSL.* SANS Institute.

Ferrigni, S. (2003). *SSL Remote Access VPNs.* SANS Institute.

Firewall.cx. (n.d.). *IPSEC - INTERNET PROTOCOL SECURITY*. Retrieved from Firewall.cx: http://www.firewall.cx/networking-topics/protocols/127-ip-security-protocol.html

Girard, J. (2011, December 12). *Magic Quadrant for SSL VPNs.* Retrieved from Gartner: http://www.sangfor.net/documentation/gartner-magic_quadrant_for_SSL_VPNs.pdf

Govcert.nl. (2009). *Telewerken.* Den Haag: Govcert.nl.

Gurung, P. (2014, December 29). *Ipsec*. Retrieved from PADAM: http://padamrajgurung.com.np/ipsec/

Hofland, I. D. (2009). *Succesfactoren van pakketselectie en -implementaties.* KPMG.

HP. (2016). *HP ArcSight Connector.* HP.

HU. (2015). Studiegids Bacholeropleiding HBO-ICT 2015-2016. In *HBO-ICT-vt-studiegids* (p. 29/111). Hogeschool Utrecht.

Kozierok, C. M. (2005, September 20). *IPSec General Operation, Components and Protocols*. Retrieved from Tcpipguide.com: http://www.tcpipguide.com/free/t_IPSecGeneralOperationComponentsandProtocols-3.htm

McKinley, H. L. (2003). *SSL and TLS: A Beginners Guide.* SANS Institute.

ntsecurity.com. (n.d.). *Barracude SSL VPN 880*. Retrieved from ntsecurity.com: http://www.ntsecurity.com/barracuda-products/barracuda-ssl-vpn/barracuda-ssl-vpn-880.html

OpenReach. (2002). *IPSec vs. SSL: Why Choose?* Woburn.

Osch, P. v. (2014, Januari 20). *prioriteiten met moscow*. Retrieved from sparkeducation.nl: http://sparkeducation.nl/prioriteiten-met-moscow/

Osman, J. H. (2008). *SSL VPN Performance Evaluation.*

Padam Gurung. (2014, December 29). Retrieved from PADAM: http://padamrajgurung.com.np/ipsec/

Palo Alto Networks. (2016). *GlobalProtect Administrator's Guide.* Santa Clara: Palo Alto Networks.

Pillai, S. (2003, Januari 15). *Understanding working secure socket layer (SSL)*. Retrieved from slashroot.in: http://www.slashroot.in/understanding-working-secure-socket-layerssl

Sheila Frankel, K. K. (2005). *Guide te IPsec VPNs.* NIST.

Sheila Frankel, P. H. (2008). *Guide to SSL VPNs.* Juli.

Steehouder, M. (2012). *Leren communiceren.* Noordhoff Uitgevers.

Verbeek, P. (2015, juni 23). *Thuiswerken: 54% werknemers doet het 1 dag per week*. Retrieved from facto.nl: http://facto.nl/thuiswerken-54-werknemers-doet-het-1-tot-2-dagen-per-week/

Watchguard. (2009). *WatchGuard SSL 100 Configuration Field Guide.* WatchGuard.

WatchGuard. (n.d.). *Appliance compare*. Retrieved from watchguard.com: http://www.watchguard.com/wgrd-products/appliances-compare/190/191/216

WatchGuard Technologies Inc. (2013, Mei 1). *WatchGuard Mobile VPN*. Retrieved from Google Play: https://play.google.com/store/apps/details?id=com.watchguard&hl=nl

4.2 Figuren

4.3 Tabellen

4.4 Bijlages

• ICT SECURITY

Plan van Aanpak

Afstudeeropdracht ICT security
Onderzoek en productselectie – SSL-VPN oplossingen

WESLEY VAN DER ZALM
1630301
VERSIE 1.3

Versiebeheer

Versie	Datum	Wijzigingen
0.1	01-02-2016	- Eerste opzet plan van aanpak. Titels voor hoofdstukken bepaald. Te beantwoorde vragen per hoofdstuk toegevoegd.
0.2	02-02-2016	- Invullen van hoofdstukken aan de hand van een overleg en aangepaste stukken uit het afstudeervoorstel. Toevoegen van bijlage “Contract afstudeeropdracht”.
0.3	03-02-2016	- Document aanvullen en aanpassen aan de hand van de kwaliteitscriteria in het afstudeerleidraad.
0.4	04-02-2016	- Herschrijven van deelvragen, aanvullen “Theoretisch kader”, toevoegen van nieuwe hoofdstukken.
0.5	05-02-2016	- Toevoegen van organogram. Teksten aangepast na doorlezen. Teksten gemarkeerd die nog geverifieerd moeten worden.
0.6	05-02-2016	- Opnieuw ingericht door problemen met opmaak.
0.7	08-02-2016	- Verwerken feedback van Bart Verhaar.
0.8	10-02-2016	- Tekstuele aanpassingen. Bijlage B toegevoegd. Laatste commentaar verwerkt na overleg.
0.9	11-02-2016	- Eindpresentatie toegevoegd aan de planning. Kwestie aangepast na gesprek met Bert Buitenhuis, Simon van den Bos en Bart Verhaar. Randvoorwaarden toegevoegd. Hoofdstuk “Scope van de opdracht” toegevoegd.
1.0	15-02-2016	- Feedback van Bert Buitenhuis en Bart Verhaar verwerkt. Document helemaal nagekeken op fouten. Bijlage E toegevoegd.
1.1	16-02-2016	- Aanpassingen na overleg met Bart Verhaar
1.2	18-02-2016	- Aanvullingen na leerteambijeenkomst van 16-02. Randvoorwaarden aangevuld, Kwestie aangepast, Scope van de opdracht aangepast en Bijlage F toegevoegd. Kopje “kwaliteitscriteria” toegevoegd.
1.3	07-03-2016	- Aanpassingen na feedback Simon van den Bos

Inhoud

1.0 Inleiding

In dit document wordt het plan van aanpak beschreven met betrekking tot de afstudeeropdracht "*Onderzoek en productselectie SSL-VPN oplossingen*". Dit document is bedoeld om een duidelijk beeld te geven van de opdracht, de uit te voeren taken en de aanpak die daarbij hoort. Dit document bevat een contract (zie bijlage D) die getekend dient te worden door de student, de docentbegeleider en bedrijfsbegeleider. Een getekend contract geeft toestemming voor de start van de opdracht. De afstudeerperiode is van februari 2016 t/m juni 2016.

1.1 Aanleiding

De laatste jaren is het SSL[1]-VPN[2] landschap stevig veranderd. Zo wordt bijvoorbeeld steeds vaker een telewerkoplossing gecombineerd met andere security oplossingen (zoals firewalls) op één systeem. Tegenwoordig willen steeds meer gebruikers een VPN verbinding maken met apparaten zoals smartphones en tablets. Motiv is op zoek naar een veilige SSL-VPN oplossing die goed past bij de nieuwe eisen en wensen die voort zijn gekomen uit de nieuwe veranderingen. De opdrachtgever wil de resultaten van deze opdracht kunnen gebruiken om een keuze voor het portfolio te maken.

1.2 De organisatie

Motiv is een ICT-security organisatie die andere organisaties voorziet van IT-beveiligingsoplossingen en –diensten. Deze maatregelen zijn nodig ter voorkoming van cybercriminaliteit, datadiefstal en datalekken. Motiv levert al sinds 1998 security-oplossingen vanuit de disciplines netwerk- en security-infrastructuur, consultancy, applicatieontwikkeling en databasetechnologie. Motiv biedt een breed scala aan 24x7 Managed Security Services en hosting. Door het eigen Security Operations Center worden cyberaanvallen, kwetsbaarheden en datalekken opgespoord, voorkomen en beperkt.

Motiv is gevestigd in IJsselstein en heeft ca. 100 medewerkers. Motiv's bedrijfsprocessen, softwareontwikkeling en Managed Security Services zijn gecertificeerd op basis van ISO9001 (kwaliteitsmanagement), ISO27001 (informatiebeveiliging) en ISO20000 (Service Management op basis van ITILv3).

[1] Secure Socket Layer: Beveiligingsprotocol voor het opzetten van een veilige verbinding. (Sheila Frankel P. H., 2008)

[2] Virtual Private Network: Techniek waarmee een verbinding kan worden gemaakt met het bedrijfsnetwerk vanaf het publieke netwerk. (Sheila Frankel P. H., 2008)

1.3 Positie van de student binnen de organisatie

Als afstudeerder val ik binnen Motiv onder de afdeling Product management. Een organogram van Motiv is bijgevoegd en te vinden in Bijlage A.

De opdrachtgever verwacht dat ik 40 uur per week bezig ben met het project. Dit zal voornamelijk op de locatie aan de Utrechtseweg in IJsselstein zijn. De opdrachtgever heeft aangegeven dat in overleg thuiswerken ook een optie is.

Gedurende mijn afstudeerperiode krijg ik een plek op de tweede verdieping bij Motiv waar ik al mijn tijd mag besteden aan de opdracht. Van mij wordt verwacht dat ik maandag tot en met vrijdag tussen 07:30 en 17:30 uur acht uren aanwezig ben. Zelf heb ik gekozen om 07:30 uur te beginnen en 16:00 uur te stoppen (dit is inclusief een half uur pauze).

2. De kwestie

In het verleden (ongeveer 10 jaar geleden) is er gekozen voor Juniper Pulse als VPN-oplossing binnen het portfolio van Motiv. Juniper Pulse wordt geleverd als product aan de klanten. Aansluitend op dit product, kan de klant kiezen voor verschillende beheerdiensten van Motiv. Deze bestaan uit:

- Easy Connect: De klant is verantwoordelijk voor de security. Motiv zorgt voor (product)ondersteuning.
- Service Connect: Het technische IT beheer van de dienst wordt volledig of gedeeltelijk door Motiv uitgevoerd. Er wordt geen beveiligingsbeheer verzorgt door Motiv.
- Full Connect: Het technische IT beheer en beveiligingsbeheer van de dienst wordt volledig door de beveiligingsexperts van Motiv uitgevoerd. (Bastiaan Bakker, 2014)

Momenteel heeft Motiv ongeveer 10 klanten in volledig beheer.

Door de jaren heen is er echter veel veranderd. Er zijn nieuwe end-points bijgekomen, VPN-oplossingen worden anders geïmplementeerd en er zijn verschillende overnames geweest. Door al deze veranderingen wordt de dienst “Veilig telewerken” niet goed meer verkocht door Motiv. Steeds vaker kiezen de klanten zelf voor een oplossing. Motiv is op zoek naar een oplossing die de dienst “Veilig telewerken” uniek maakt en er voor zorgt dat de dienst vaker wordt afgenomen.

2.1 Doelstelling

Het doel is om aan de hand van de gestelde eisen en wensen een productselectie te maken. Uiteindelijk worden er naast de huidige oplossing, één of twee vernieuwde oplossingen gebouwd in een testomgeving (*proof of concept*). Het aantal gekozen oplossingen hangt af van de uiteindelijke score ten opzichte van de eisen en wensen. Wanneer er één vernieuwde oplossing veel meer scoort dan de rest, is het niet nodig om nog een andere oplossing te testen aan de hand van een *proof of concept*.

Uiteindelijk moet er aan de hand van een *proof of concept* een keuze worden gemaakt voor een oplossing. Dit kan ook de huidige oplossing van Motiv zijn.

De gekozen oplossing wordt gepresenteerd aan Motiv in een eindpresentatie. In deze eindpresentatie wordt uitgelegd waarom deze oplossing de beste keuze is voor Motiv en haar klanten en hoe ik tot die keuze ben gekomen. Het doel van de opdracht is om een advies aan Motiv te geven, over welke oplossing het beste bij de eisen en wensen past. De productmanager van Motiv en tevens opdrachtgever (Bart Verhaar) wil aan de hand van mijn onderzoek een keuze kunnen maken voor het beste product.

De opdracht is voltooid wanneer er een goed onderbouwd advies kan worden gegeven aan de opdrachtgever.

2.2 Type opdracht

De beschreven opdracht valt onder het type advies/ontwerp. Het is de bedoeling dat er een advies wordt gegeven over een eventuele vernieuwde SSL VPN-oplossing. De opdrachtgever heeft aangegeven een advies te willen waar een beslissing op genomen kan worden. Voordat er een

advies wordt gegeven, worden er eerst testopstellingen gebouwd (*proof of concept*). Het maken van een implementatieplan valt buiten de scope van de opdracht.

2.3 Scope van de opdracht

De beschreven opdracht betreft een productselectie voor een vernieuwde SSL VPN-oplossing. Eisen en wensen vanuit ISO-normeringen vallen buiten de scope van het onderzoek. De oplossing moet passen binnen het huidige portfolio van Motiv. Dit betekent dat diensten die gekoppeld zijn aan de dienst “Veilig telewerken” ongewijzigd dienen te blijven. Diensten die hieronder vallen zijn bijvoorbeeld “Sterke authenticatie” en “Beheerder Firewall”.

Uit een mailwisseling met Bart Verhaar (Zie bijlage F) is gebleken dat er in de eisen en wensen, rekening gehouden moet worden met cloud services. Een eis/wens (nader te bepalen) wordt dat de SSL VPN-oplossing de protocollen die toegang naar cloud services bieden, ondersteunt.

3. Onderzoeksvraag

Momenteel luidt mijn hoofdvraag als volgt:

- ***'Welke SSL VPN-oplossing past het best bij de huidige eisen en wensen van Motiv en van haar klanten?'***

Met het oog op het doel van deze opdracht is er gekozen voor bovenstaande onderzoeksvraag. Medewerkers van Motiv kennen de behoeften van hun klanten en nemen dit mee in het stellen van eisen en wensen. De impact van nieuwe ontwikkelingen wordt meegenomen in het onderzoek.

3.1 Deelvragen

Om de hoofdvraag te kunnen beantwoorden is er gekozen voor onderstaande deelvragen. De deelvragen staan in chronologische volgorde en dienen één voor één beantwoord te worden. De gekozen deelvragen zijn gebaseerd op de KPMG-pakketselectiemethodiek zoals beschrijven in het "Theoretisch kader" (Hoofdstuk 11) (Hofland, 2009). Voor elke deelvraag zijn er concept-subdeelvragen gedefinieerd. Deze subdeelvragen met de toe te passen methoden om informatie te verzamelen vindt u in bijlage B.

A. Wat zijn de '*Key Criteria*' van Motiv en haar klanten en welke SSL VPN-oplossingen voldoen daaraan?

Aan het begin van het onderzoek moet duidelijk worden waar de oplossing op zijn minst aan moet voldoen. '*Key Criteria'* kan ook gezien worden als de "Must have" uit het MoSCoW model (Osch, 2014). Dat betekent dat zonder deze gestelde eis(en) het product niet bruikbaar is.

Als de '*Key Criteria'* vast staan, kan er een longlist gemaakt worden van de oplossingen die hier aan voldoen.

B. Wat zijn de eisen en wensen van Motiv en haar klanten en hoe belangrijk zijn ze?

Nu er sprake is van een longlist, is het de bedoeling om tot een kleinere selectie te komen. In deze deelvraag is de eerste stap om alle eisen en wensen van de opdrachtgever boven tafel te krijgen. Dit geldt voor zowel functionele eisen, business eisen en technische eisen.

Wanneer er een lijst is van de verschillende eisen, moeten deze worden gecategoriseerd en geprioriteerd. Het toekennen van een prioriteit is bepalend voor de wegingsfactor van de score. De prioriteit wordt bepaald aan de hand van het MoSCoW model. (Osch, 2014)

C. Welke twee oplossingen scoren het beste op de vastgestelde eisen en wensen?

Aan de hand van de voorgeselecteerde oplossingen en de vastgestelde eisen, kan er een scorematrix worden gemaakt. Elke oplossing wordt hierin beoordeeld op de vastgestelde eisen en wensen doormiddel van een score. Wanneer een eis belangrijk is, is de scoringsfactor hoger dan van een wens die minder belangrijk is.

Wanneer de gehele scorematrix is ingevuld, worden er twee oplossingen geselecteerd.

D. Hoe zien de geselecteerde en de huidige SSL VPN-oplossingen er in een testomgeving uit?

Er wordt een technisch ontwerp gemaakt voor de geselecteerde oplossing en de huidige oplossing van Motiv. Deze dient tijdig goedgekeurd te worden door de opdrachtgever om gebruik te kunnen maken van het lab. Als de ontwerpen zijn goedgekeurd, worden de testomgevingen opgebouwd in het lab.

E. Hoe scoren de SSL VPN-oplossingen in een testomgeving?

Aan de hand van de gestelde eisen en wensen wordt er een testformulier gemaakt. Als de testomgevingen zijn opgezet, kan het testformulier worden ingevuld. De resultaten zijn het antwoord op deze deelvraag. Het resultaat van deze test wordt gebruikt bij het beantwoorden van de hoofdvraag.

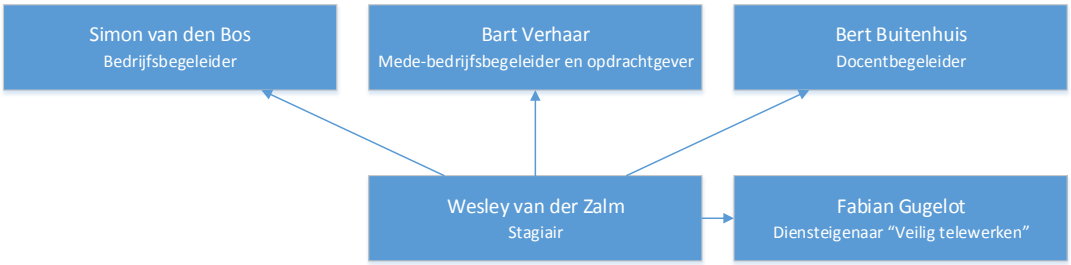
4.0 De projectorganisatie

Tot op heden zijn de actoren uit figuur 10 bekend. De opdracht is afkomstig van Bart Verhaar. Bart Verhaar is tevens mijn mede-bedrijfsbegeleider. Simon van den Bos is hierin mijn bedrijfsbegeleider en begeleidt de afstudeerder waar nodig. Tevens formuleren Simon van den Bos en Bart Verhaar de business requirements.

Fabian Gugelot is Security Engineer bij Motiv en diensteigenaar van de “Veilig telewerken” dienst van Motiv. Met Fabian kan ik contact opnemen voor de technische kant van het project. Door middel van een interview kan ik bij hem de technische eisen en wensen formuleren.

Bert Buitenhuis is door de Hogeschool Utrecht toegewezen als docentbegeleider gedurende het project.

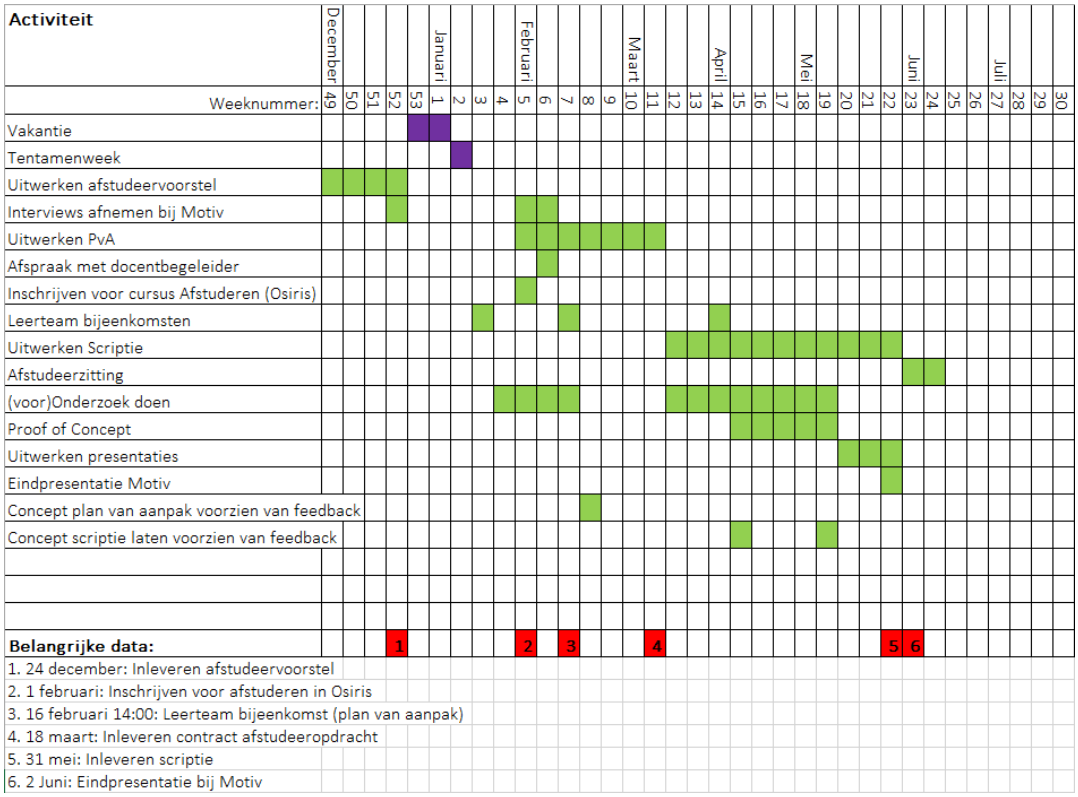
De Stagiair is verantwoordelijk voor het onderzoek en de resultaten van de opdracht.



Figuur 10 De projectorganisatie

5.0 Planning & werkzaamheden

Voor mijn afstudeerperiode heb ik een schematische planning gemaakt (zie figuur 11). Dit is nodig om een goed overzicht te creëren van de verschillende fasen en deadlines goed in de gaten te houden. Verder vind u in dit hoofdstuk de daarbij horende producten, activiteiten, deadlines en urenverdeling.



Figuur 11 Planning

5.1 Activiteitenbeschrijving, producten en resultaten

Het is belangrijk om een goed overzicht te maken van de taken/activiteiten die een rol gaan spelen in het project en een inschatting van de tijd die het gaat kosten. Om deze reden beschrijf ik per fase de producten, activiteiten, resultaten, deadlines en geschatte uren.

5.1.1 Voorbereiding

In de voorbereiding maak ik kennis met Motiv. Om een goed beeld van de opdracht te krijgen, neem ik zo snel mogelijk contact op met Bart Verhaar en Simon van den Bos. Na het stellen van de juiste vragen, kan ik beginnen met het schrijven van een plan van aanpak. Tijdens het schrijven van mijn plan van aanpak ga ik onder andere op zoek naar wetenschappelijke bronnen en methoden die ik kan gebruiken voor mijn afstudeeropdracht.

In dezelfde periode dien ik mij in te schrijven voor het afstuderen in Osiris en een afspraak te maken met mijn docentbegeleider Bert Buitenhuis. Tijdens deze afspraak neem ik mijn concept plan van aanpak mee voor eventuele opmerkingen.

Er staat een leerteambijeenkomst gepland op school om mijn plan van aanpak te laten beoordelen door studenten uit hetzelfde leerteam. Zelf ga ik ook andere plannen van aanpak bekijken van medestudenten en deze voorzien van mijn feedback.

Activiteiten	*Uren*
Kennismaken, oriëntatie	40
Vooronderzoek doen	80
Schrijven, aanpassen en verbeteren plan van aanpak	120
Inschrijven Osiris	1
Leerteambijeenkomsten	10
Afspraak docentbegeleider	4
Overleggen	10
Totaal	**265**

Tabel 32 Urenverdeling voorbereiding

Bovengenoemde activiteiten moeten leiden tot een goedgekeurd plan van aanpak en een getekend afstudeeropdracht contract. De deadline hiervoor is 18-03-2016.

5.1.2 Onderzoek, bouwen en testen

Deze fase staat voor het uitvoeren van de opdracht. Deze fase gaat van start wanneer het contract uit de voorbereiding door de docentbegeleider, bedrijfsbegeleider en de student is getekend.

Centraal staat de onderzoeksvraag uit hoofdstuk 3. Om deze te beantwoorden zijn er activiteiten per (sub)deelvraag nodig. Alle activiteiten in tabel 33 worden verwerkt in de scriptie.

Wederom is er een leerteambijeenkomst gepland. Dit moment is een week voor het opleveren van een conceptversie van de scriptie. Op deze dag wordt de scriptie al voorzien van feedback door medestudenten uit het team.

Activiteiten	*Uren*
Vaststellen Key Criteria	10
Maken van longlist a.d.h.v. Key Criteria	30
Vaststellen eisen en wensen	40
Eisen en wensen prioriteren	10
Maken van shortlist	40
Vaststellen van de twee best scorende oplossingen	20
Proof of concept voorbereiden	40
Proof of concept uitvoeren	160
Opstellen en invullen testrapport	40
Beantwoorden van de hoofdvraag	20
Schrijven van overige rapportages	50
Totaal	**460**

Tabel 33 Urenverdeling onderzoek, bouwen en testen

Deze fase is afgerond wanneer de hoofdvraag is beantwoord en de scriptie afgerond is. De deadline hiervoor is 31-05-2016.

5.1.4 Oplevering

Alle resultaten uit het onderzoek worden verzameld. In deze fase wordt er een eindpresentatie gemaakt voor het stagebedrijf Motiv en voor de Hogeschool Utrecht. De data voor de presentatie en de hoorzitting moeten nog worden vastgesteld.

Activiteiten	*Uren*
Verzamelen en samenvatten van resultaten	30
Opbouwen van presentatie en teksten	40
Presenteren	8
Totaal	**78**

Tabel 34 Urenverdeling oplevering

5.2 Studielast

Voor het afstuderen vallen er 30 studiepunten te behalen voor de student. De studielast van 1 EC komt overeen met 28 studie(klok)uren (inclusief contacttijd). (HU, 2015)

Dit betekent dat het afstuderen (30*28=) 840 uur gaat kosten. Hiervan ben ik 800 uur aanwezig bij mijn stagebedrijf. De overige uren zijn gedeeltelijk reeds besteed aan verwerven van een opdracht en het schrijven van een afstudeervoorstel. Ook staan er nog afspraken op school gepland die gedeeltelijk buiten de werktijden van Motiv vallen.

Deze uren zijn als volgt verdeeld:

Activiteiten	*Uren*
Verwerven opdracht	20
Schrijven afstudeervoorstel	20
Voorbereiding afstuderen	265
Uitvoering	460
Oplevering	78
Totaal	**843**

Tabel 35 Totale uren afstudeerproject

6. Vereiste vakkennis

Om de opdracht uit te kunnen voeren, dient de student kennis te hebben van:

- Professional skills

Het is belangrijk om kennis te hebben van een systematische aanpak voor het schrijven van een document.

- Onderzoeksvaardigheden

Voor het doen van een onderzoek zijn onderzoeksvaardigheden nodig. De bronnen moeten passen bij het onderzoek en feitelijk juist zijn.

- Werking van SSL VPN

Om een gevoel bij de opdracht te krijgen, is het nodig om de werking van SSL VPN te kennen. Dit heeft vooral betrekking op het technische gedeelte. Deze kennis is nodig om een *proof of concept* te kunnen maken.

- Werking van firewalls

SSL VPN oplossingen worden vaak gecombineerd met firewalls. Met het bouwen van een *proof of concept* is deze kennis dus vereist.

- Algemene technische kennis (voor systeem en netwerkbeheer)

Er moeten goede wedervragen gesteld worden wanneer er gevraagd wordt naar technische eisen en wensen. Hiervoor is een wat algemenere technische kennis nodig.

- Kennis van productselectie

Gedurende het project moet ik mij een methode eigen maken om op een goede manier tot een goed resultaat te komen.

7. Risicoanalyse

Het is goed om van te voren te bedenken wat mijn afstuderen in gevaar zou kunnen brengen. Als er risico's zijn die ik zelf in de hand heb, dan kan ik er vast alles aan doen om het niet zo ver te laten komen.

De risico's:

- Miscommunicatie

Dit heeft betrekking op de opdrachtgever, docentbegeleider, bedrijfsbegeleider en de student. De student staat hierin centraal aangezien hij met allen contact heeft en duidelijkheid moet creëren. Miscommunicatie kan bijvoorbeeld leiden tot het verkeerd formuleren van een opdracht door de student. De bedrijfsbegeleider zou zo een ander beeld van de opdracht kunnen krijgen dan de opdrachtgever.

- Geen afgebakende opdracht

Wanneer een opdracht niet genoeg is afgebakend, kan het zo zijn dat de school meer van de student verwacht dan dat er daadwerkelijk wordt opgeleverd. Dit heeft de student wederom zelf in de hand.

- Te weinig tijd

Als een opdracht complexer blijkt te zijn dan hij is, kan er sprake zijn van tijdsgebrek. Dit gaat vaak samen met een slechte voorbereiding en planning.

- Te weinig kennis

De student heeft te weinig kennis om de opdracht tot een goed einde te brengen. Dit kan het gevolg zijn wanneer de student te weinig onderzoek doet.

- Te weinig aandacht vanuit Motiv

Dit kan gebeuren wanneer bijvoorbeeld een bedrijfsbegeleider geen tijd voor mij heeft, omdat hij te druk is met eigen werkzaamheden. Ook kan dit gebeuren wanneer de student zelf niet aan de bel trekt wanneer er vragen opduiken.

- Storing/problemen met het lab

Wanneer ik aan een testopstelling wil gaan bouwen, kan het zijn dat het lab niet beschikbaar is vanwege bijvoorbeeld een stroomstoring. Dit kan vertraging opleveren.

- Beschikbaarheid van software

Bij het opstellen van een *proof of concept* maak ik gebruik van software. Hiervoor moeten (wanneer het geen open source oplossing is) licenties worden aangeschaft. Een eventueel risico is dat Motiv de licenties niet wil aanschaffen.

- Beschikbaarheid van hardware

Bij het opstellen van een *proof of concept* moet ik beschikken over de juiste hardware. Voor het bouwen moet ik dus een inventarisatie maken van het lab. Het risico bestaat dat ik hardware nodig heb waar Motiv niet over beschikt.

8. Randvoorwaarden

Om de opdracht goed te laten verlopen en de risico's te beperken zijn onderstaande randvoorwaarden opgesteld.

- Vragen van de student aan de docentbegeleider, bedrijfsbegeleider, opdrachtgever en diensteigenaar van de dienst "Veilig telewerken" dienen binnen 3 werkdagen beantwoord te zijn. Dit geldt ook voor vragen aan de student.
- Licenties en apparatuur wordt door de opdrachtgever op aangeven van de student geleverd.
- Gedurende de afstudeerperiode is er een werkplek beschikbaar binnen het stagebedrijf.
- Gedurende de afstudeerperiode heeft de student toegang tot het netwerk van Motiv.
- Bij tijdig aangeven door de student is het lab beschikbaar voor het bouwen van testopstellingen.
- De gekozen oplossing moet aansluiten op de diensten "Sterke authenticatie" en "Beheerde firewall".
- Aanpassingen van de diensten "Sterke authenticatie" en "Beheerde firewall" vallen buiten de scope van dit project.
- Het implementeren of het schrijven van een implementatieplan vallen buiten de scope van dit project.
- Wanneer een leverancier binnen een week geen reactie geeft op de gestelde vragen, wordt deze uitgesloten van het onderzoek.
- Er is elke week een moment van overleg met de opdrachtgever.
- Voor het nakijken van een concept scriptie staat 7 werkdagen.
- De student heeft de 40 uur die hij in een week aanwezig is, volledig beschikbaar voor de afstudeeropdracht.
- Er is een mogelijkheid tot thuiswerken.

9. Eindproducten/mijlpalen

Het eindresultaat bestaat uit de volgende op te leveren producten:

- Afstudeervoorstel

Document waarin ik mijn opdracht en stagebedrijf beschrijf met als doel goedkeuring te krijgen voor mijn verworven opdracht.

- Plan van Aanpak

Document waarin de opdracht verder wordt uitgelicht. Het moet onder andere duidelijk zijn wat het doel van de opdracht is, wanneer dat doel bereikt is en hoe ik dat ga bereiken. Ter voorbereiding op het onderzoek wordt er al een hoofdvraag en deelvragen geformuleerd. Het plan van aanpak geldt als contract en dient getekend te worden door de student, bedrijfsbegeleider en docentbegeleider.

- Scriptie

Het verslag waar aan de hand antwoorden op deelvragen, de hoofdvraag beantwoord kan worden. Dit document bevat onder andere literatuuronderzoek, interviews en testresultaten.

- Testplan

Document waar testvragen zijn gemaakt aan de hand van de gestelde eisen en wensen door Motiv. Na het maken van een *proof of concept* wordt het testplan ingevuld. De resultaten van het testplan worden gebruikt voor een conclusie en het beantwoorden van de hoofdvraag.

- *Proof of Concept*

Het maken en testen van een proefopstelling. De proefopstelling wordt gemaakt in het lab van Motiv en is bedoeld om een aantal cruciale functies te testen. Dit gebeurt met de geselecteerde en huidige oplossingen. Het lab beschikt over een verbinding naar het internet om een realistisch beeld te kunnen verkrijgen.

- Eindpresentatie

De gekozen oplossing wordt gepresenteerd in de eindpresentatie. In deze presentatie wordt ook uitgelegd hoe ik tot de keuze ben gekomen.

9.1 Kwaliteitscriteria

Alle eindproducten die worden opgeleverd, voldoen aan de volgende kwaliteitscriteria:

- In geval van onderzoek, zijn conclusies gebaseerd op onafhankelijke, wetenschappelijke bronnen;
- De op te leveren eindproducten zijn geschreven in correct Nederlands;
- De kwaliteit van de op te leveren eindproducten komen overeen met het opleidingsniveau (HBO);
- Bronnen worden vermeld volgens APA;
- Bij gebruik van bronnen, dienen deze valide te zijn;
- Schriftelijke eindproducten zullen voldoen aan de richtlijnen van de afstudeerleidraad en het boek *Leren communiceren* van Steehouder.

10. Actoren

Binnen mijn afstudeeropdracht zijn de volgende actoren bekend:

Student
Naam: Wesley van der Zalm
E-mail: wesleyvdzalm@gmail.com / wesley.vanderzalm@student.hu.nl
Telefoonnummer: 0634324833
LinkedIn: http://nl.linkedin.com/in/wesleyvdzalm

Bedrijfsbegeleider
Naam: Simon van den Bos
E-mail: simon.vandenbos@motiv.nl
Telefoonnummer: 0620025630
LinkedIn: https://nl.linkedin.com/in/simon-van-den-bos-a5a4a9/nl
Opleidingsniveau: Universiteit (Rotterdam University of Applied Sciences (1986-1990), Technical University in Utrecht(1991-1992))

Mede-bedrijfsbegeleider
Naam: Bart Verhaar
E-mail: bart.verhaar@motiv.nl
Telefoonnummer: 030 6877 007
LinkedIn: https://nl.linkedin.com/in/bartverhaar/nl

Docentbegeleider
Naam: Bert Buitenhuis
E-mail: bert.buitenhuis@hu.nl
Telefoonnummer: 08848108195 / 0653737411
LinkedIn: https://nl.linkedin.com/in/bbuitenhuis/nl

10.1 Algemeen communicatieplan

Om er voor te zorgen dat de communicatie tussen de student en overige bovengenoemde actoren goed verloopt, wordt er een communicatieplan opgesteld.

Om de voortgang van het project te bepalen en de gelegenheid te krijgen om vragen te stellen, is het belangrijk dat er regelmatig contact is met de bedrijfsbegeleider en mede-bedrijfsbegeleider. Er is afgesproken om wekelijks om de tafel te gaan zitten om de voortgang van de opdracht te bespreken. Dit overleg staat elke woensdagochtend gepland. Gedurende de rest van de week verzamel ik vragen die geen hoge nood hebben. Wanneer ik vast loop op een vraag kan ik deze direct stellen. Naast het wekelijkse overleg is er ook mailcontact.

Naast het contact met de docentbegeleider en de bedrijfsbegeleider, zijn er ook contactmomenten met medestudenten. Dit contact vind plaats tijdens de leerteambijeenkomsten. Er zijn drie leerteambijeenkomsten waarvan er al één is geweest.

De drie momenten zijn:

- Startsessie leerteams (25-01-2016)
- Plan van aanpak sessie (16-02-2016)
- Scriptie sessie (wordt 16-02-2016 gepland)

Tijdens de startsessie zijn de leerteams samengesteld. Deze zijn zo goed mogelijk samengesteld op overeenkomsten zoals opleiding en type opdracht. Tijdens de startsessie hebben de studenten in het team elkaars afstudeervoorstel en concept hoofdvraag voorzien van feedback. Als afsluiting is er een nieuwe afspraak gemaakt om het concept plan van aanpak met elkaar door te nemen. Deze sessie is gepland op 16-02-2016 om 14:00. Aan het eind van deze sessie wordt er een afspraak gemaakt voor de scriptie sessie.

10.2 Communicatie bij ziekte, afwezigheid of verzuim volgens stageovereenkomst

In het geval van ziekte of afwezigheid wegens een dringende reden, alsmede van hervatting na ziekte of na afwezigheid, stelt de stagiair de stagegever en de school onverwijld op de hoogte. De stagegever informeert de school direct in geval van verzuim van de stagiair. Zodra de afwezigheid een zodanig betekenende omvang heeft dat er naar het oordeel van de school een onvoldoende basis is om de stage nog te kunnen beoordelen zullen partijen trachten tot nadere afspraken te komen (b.v. overeenkomstige verlenging van de oorspronkelijke afspraken). (Artikel 6 Stageovereenkomst, 2016)

11. Theoretisch kader

Gedurende de opdracht is het aan mij de taak om een SSL VPN-oplossing te kiezen die het beste aansluit bij de behoefte van de opdrachtgever en de klanten van Motiv. Een belangrijke stap in dit project is het maken van een productselectie. Hierbij maak ik gebruik van de methode die is beschreven door het bedrijf KPMG (Hofland, 2009). KPMG is een bedrijf dat onder andere advies geeft aan andere organisaties op gebied van ICT. In figuur 12 vind u het model dat door KPMG is ontwikkeld.

Figuur 12 KPMG-pakketselectiemethodiek

Door tijdens de opdracht gebruik te maken van de KPMG-pakketselectiemethodiek, kan ik systematisch te werk gaan. Voor de afstudeeropdracht valt de laatste stap (contracteren) buiten de scope.

Voor het opstellen van een programma van eisen, wordt er gebruik gemaakt van de MoSCoW-methode. De MoSCoW-methode is een manier om prioriteiten te stellen bij de eisen en wensen. (Osch, 2014)

Voor het testen van de testopstellingen, maak ik gebruik van het “Template Testplan” van de ASL BiSL foundation.

Verder staan nog nader te onderzoeken bronnen voor de opdracht in de voorlopige literatuurlijst. Deze lijst vind u in bijlage E.

12. Bronnen / literatuurlijst

An overview of the SSL or TLS handshake. (2014). Opgehaald van ibm.com: http://www-01.ibm.com/support/knowledgecenter/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm?lang=en

Artikel 6 Stageovereenkomst. (2016, Februari). *Stageovereenkomst*. IJsselstein: Motiv ICT Security.

ASL BiSL Foundation. (2006, februari 1). *Downloads.* Opgehaald van ASLBiSLFoundation.org.nl: http://aslbislfoundation.org/nl/

Bastiaan Bakker, P. S. (2014, Mei 20). *Fabrikanten documenten.* Opgehaald van Motown: https://motown.motiv.nl/Site/Fabrikanten/Documenten%20met%20accreditatie/DC%20Cloud%20en%20datacenter%20security%20diensten%201.2.pdf

bestuurszaken.be. (sd). *Definitie telewerk*. Opgehaald van bestuurzaken.be: https://www.bestuurszaken.be/definitie-telewerk

Crawford, J. T. (2011, April 14). *How VPNs Work*. Opgehaald van Howstuffworks: http://computer.howstuffworks.com/vpn.htm

DeBeasi, P. (2014, december 22). *Vendor Rating: Citrix.* Opgehaald van Gartner: http://www.gartner.com/document/2949722?ref=solrAll&refval=164021515&qid=6187faaf3baba1d3b3713c6d8d916a63

Eveleens, W. (2006). *Rendement en risico's van telewerken.* Den Haag: Sdu Uitgevers.

Fabian Gugelot, S. v. (2016, februari 24). Eisen en wensen voor een SSL VPN oplossing. (W. v. Zalm, Interviewer)

Faura, X. G. (2005). *Understanding VPN tunnels over SSL.* SANS Institute.

Ferrigni, S. (2003). *SSL Remote Access VPNs.* SANS Institute.

Firewall.cx. (sd). *IPSEC - INTERNET PROTOCOL SECURITY*. Opgehaald van Firewall.cx: http://www.firewall.cx/networking-topics/protocols/127-ip-security-protocol.html

Girard, J. (2011, December 12). *Magic Quadrant for SSL VPNs.* Opgehaald van Gartner: http://www.sangfor.net/documentation/gartner-magic_quadrant_for_SSL_VPNs.pdf

Govcert.nl. (2009). *Telewerken.* Den Haag: Govcert.nl.

Gurung, P. (2014, December 29). *Ipsec*. Opgehaald van PADAM: http://padamrajgurung.com.np/ipsec/

Hofland, I. D. (2009). *Succesfactoren van pakketselectie en -implementaties.* KPMG.

HP. (2016). *HP ArcSight Connector.* HP.

HU. (2015). Studiegids Bacholeropleiding HBO-ICT 2015-2016. In *HBO-ICT-vt-studiegids* (p. 29/111). Hogeschool Utrecht.

Kozierok, C. M. (2005, September 20). *IPSec General Operation, Components and Protocols*. Opgehaald van Tcpipguide.com: http://www.tcpipguide.com/free/t_IPSecGeneralOperationComponentsandProtocols-3.htm

McKinley, H. L. (2003). *SSL and TLS: A Beginners Guide.* SANS Institute.

ntsecurity.com. (sd). *Barracude SSL VPN 880*. Opgehaald van ntsecurity.com: http://www.ntsecurity.com/barracuda-products/barracuda-ssl-vpn/barracuda-ssl-vpn-880.html

OpenReach. (2002). *IPSec vs. SSL: Why Choose?* Woburn.

Osch, P. v. (2014, Januari 20). *prioriteiten met moscow*. Opgehaald van sparkeducation.nl: http://sparkeducation.nl/prioriteiten-met-moscow/

Osman, J. H. (2008). *SSL VPN Performance Evaluation.*

Padam Gurung. (2014, December 29). Opgehaald van PADAM: http://padamrajgurung.com.np/ipsec/

Palo Alto Networks. (2016). *GlobalProtect Administrator's Guide.* Santa Clara: Palo Alto Networks.

Pillai, S. (2003, Januari 15). *Understanding working secure socket layer (SSL)*. Opgehaald van slashroot.in: http://www.slashroot.in/understanding-working-secure-socket-layerssl

Sheila Frankel, K. K. (2005). *Guide te IPsec VPNs.* NIST.

Sheila Frankel, P. H. (2008). *Guide to SSL VPNs.* Juli.

Steehouder, M. (2012). *Leren communiceren.* Noordhoff Uitgevers.

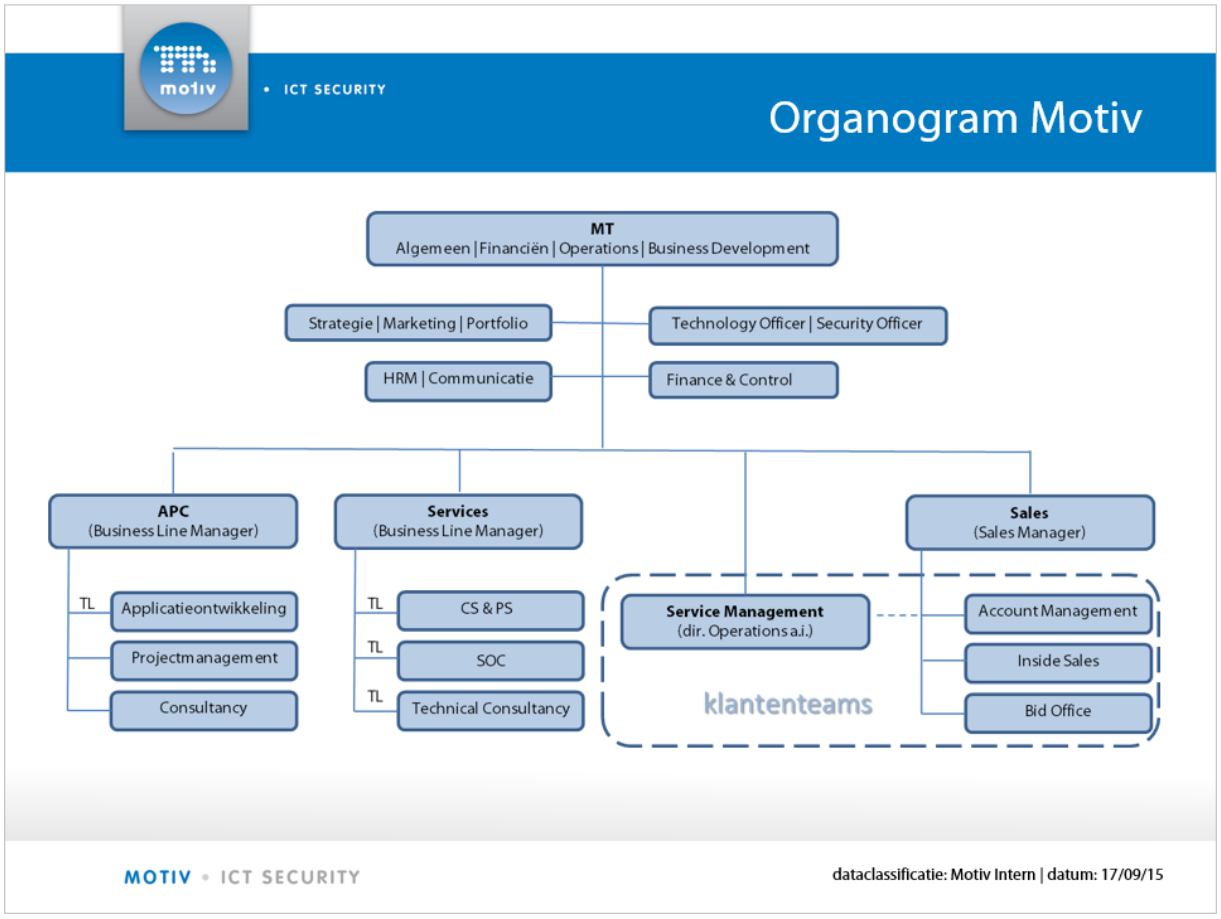
Verbeek, P. (2015, juni 23). *Thuiswerken: 54% werknemers doet het 1 dag per week*. Opgehaald van facto.nl: http://facto.nl/thuiswerken-54-werknemers-doet-het-1-tot-2-dagen-per-week/

Watchguard. (2009). *WatchGuard SSL 100 Configuration Field Guide.* WatchGuard.

WatchGuard. (sd). *Appliance compare*. Opgehaald van watchguard.com: http://www.watchguard.com/wgrd-products/appliances-compare/190/191/216

WatchGuard Technologies Inc. (2013, Mei 1). *WatchGuard Mobile VPN*. Opgehaald van Google Play: https://play.google.com/store/apps/details?id=com.watchguard&hl=nl

Bijlage A Organogram Motiv



Figuur 13 Organogram Motiv

Bijlage B Subdeelvragen met methoden

Deelvraag 1: Wat zijn de '*Key Criteria*' van Motiv en haar klanten en welke SSL VPN-oplossingen voldoen daaraan?

	Subdeelvraag	**Methode dataverzameling**
1.1	Wat is en hoe werkt een SSL VPN-oplossing?	Bestuderen van literatuur.
1.2	Wat zijn de '*Key Criteria*' vanuit business oogpunt?	Vragen aan Simon van den Bos en/of Bart Verhaar.
1.3	Wat zijn de '*Key Criteria*' vanuit technisch oogpunt?	Vragen aan Fabian Gugelot.
1.4	Welke SSL VPN-oplossingen zijn er op de markt?	Bestuderen van internetbronnen.

Deelvraag 2: Wat zijn de eisen en wensen van Motiv en haar klanten en hoe belangrijk zijn ze?

	Subdeelvraag	**Methode dataverzameling**
2.1	Welke vragen moeten er aan wie gesteld worden om de eisen en wensen te bepalen?	Bestuderen van literatuur en overige bronnen die gelijkenissen tonen met dit project.
2.2	Wat zijn de eisen en wensen van Motiv en haar klanten?	Fabian Gugelot, Simon van de Bos en/of Bart Verhaar interviewen.
2.3	Hoe belangrijk zijn de eisen en wensen van Motiv en haar klanten?	Bestuderen van prioriteringsmethoden

Deelvraag 3: Welke twee oplossingen scoren het beste op de vastgestelde eisen en wensen?

	Subdeelvraag	**Methode dataverzameling**
3.1	Hoe wordt de score van de oplossingen bepaald?	Bestuderen van scoringsmethoden en product/pakketselectiemethoden.
3.2	Hoe scoren de oplossingen uit de longlist op de vastgestelde eisen en wensen?	Resultaten van subdeelvraag 2.3 en 3.1.

Deelvraag 4: Hoe zien de geselecteerde en de huidige SSL VPN-oplossingen er in een testomgeving uit?

	Subdeelvraag	**Methode dataverzameling**
4.1	Hoe ziet het technisch en functioneel ontwerp van de huidige SSL VPN-oplossing er uit?	Bestuderen van literatuur en interne bronnen bij Motiv. Vragen aan Fabian Gugelot.
4.2	Hoe zien de technisch en functioneel ontwerpen van de geselecteerde SSL VPN-oplossingen er uit?	Bestuderen van literatuur.
4.3	Wat is er nodig om de SSL VPN-oplossingen op te zetten in een testomgeving?	Manuals van leveranciers bestuderen.
4.4	Hoe zijn de testopstellingen geconfigureerd?	Configuratie van de opstellingen in de *proof of concept*.

Deelvraag 5: Hoe scoren de SSL VPN-oplossingen in een testomgeving?

	Subdeelvraag	**Methode dataverzameling**
5.1	Waar moeten de testopstellingen op worden getest?	Antwoord van deelvraag 2. Template testplan van ASL BiSL Foundation.
5.2	Hoe ziet het resultaat van de test er per opstelling uit?	Resultaten uit de *proof of concept*.

Bijlage C Afstudeeropdracht

Afstudeeropdracht ICT security
Onderzoek en productselectie – SSL-VPN oplossingen

Regio: Utrecht **Locatie**: IJsselstein

Achtergrondinformatie

Motiv is één van de meest toonaangevende ICT security bedrijven van Nederland. Zij is ISO gecertificeerd tegen de normen 9001, 27001 en 2000-2012. Naast het leveren van consultancy op het gebied van informatiebeveiliging, het bouwen en veilig hosten van applicaties, levert Motiv ook ICT security diensten vanuit haar datacenterlocaties en vanuit de cloud. De tendens bij klanten is om ICT beveiliging als dienst af te nemen in plaats van zelf dure en complexe systemen in huis te halen en deze te beheren.

Steeds meer bedrijven bieden hun medewerkers de mogelijkheid om via een veilige telewerkoplossing toegang te krijgen tot applicaties in het bedrijfsnetwerk. Motiv levert hiervoor SSL-VPN telewerkoplossingen, vaak in combinatie met 2-factor authenticatie.

De telewerkoplossing past beveiligingsmaatregelen toe op end-point communicatie vanuit internet naar applicaties in het bedrijfsnetwerk. Een end-point kan een PC of Mac zijn, maar is ook steeds vaker een tablet of smartphone. Voordat toegang wordt gegeven tot bedrijfsapplicaties, wordt het end-point gescand op aanwezige dreigingen.

Afgelopen jaren hebben security leveranciers veel aandacht besteed aan het consolideren van verschillende security oplossingen op één systeem. Ook de telewerkoplossing wordt steeds vaker op één platform gecombineerd met andere security oplossingen en mede hierdoor is het SSL-VPN landschap flink veranderd.

Opdracht

Met deze opdracht wil Motiv laten onderzoeken wat tegenwoordig van een telewerkplatform verwacht wordt en welke leveranciers hierin meegroeien. Wat kunnen we in de toekomst verwachten op dit onderwerp en welke functie krijgt een telewerkplatform in relatie tot threat detectie en preventie?

Je start met een aantal interviews binnen Motiv om de scope van het project en de eisen en wensen vast te stellen. Daarna ga je inventariseren welke spelers de leiders zijn in dit marktsegment en hoe de SSL-VPN telewerkoplossingen scoren ten opzichte van elkaar. Ook het huidige leveringsprogramma van Motiv neem je onder de loep.

Nadat je de twee beste oplossingen hebt geselecteerd, worden deze in een *proof of concept* technisch aan een onderzoek onderworpen.

Je eindigt met een presentatie van de resultaten binnen Motiv en je bent in staat om je adviezen te verdedigen.

Je voert de opdracht uit in nauwe samenwerking met ervaren consultants en engineers van Motiv.

Opleiding: HBO/Universiteit

Vergoeding: € 450 per maand

Aanvang: in samenspraak

Contact: Iris Swartjes, HR Manager, 030-6877007

Duur: 5 maanden

Bijlage D Contract afstudeeropdracht

Contract afstudeeropdracht
Institute for ICT
Nijenoord 1, 3552 AS, UTRECHT

Naam student :

Afstudeerrichting: Variant: voltijd / deeltijd / duaal

Adres student :

Postcode / Woonplaats student:

Studentnummer :

Telefoonnummer privé :

E-mailadres :

Naam bedrijf (afstuderen) :

Adres bedrijf :

Postcode / Woonplaats bedrijf :

Naam bedrijfsbegeleider :

Telefoonnummer bedrijfsbegeleider :

E-mailadres bedrijfsbegeleider :

Beoogde maand van afstuderen : *maand en jaar invullen*

Geheimhouding geaccordeerd door HU op : *indien van toepassing*

Inleverdata van twee concept-scripties : /

Beschrijving van de afstudeeropdracht

Geef hier in enkele zinnen weer wat de afstudeeropdracht inhoudt.

Hoofd- een deelvragen van het uit te voeren onderzoek

Noteer hier de hoofdvraag met deelvragen van het onderzoek dat voor het uitvoeren van de afstudeeropdracht moeten worden uitgevoerd.

Op te leveren producten

Beschrijf hier de producten die aan het einde van het afstudeerproject moeten zijn opgeleverd.

Akkoordverklaringen

Ondergetekenden verklaren akkoord te gaan met de afstudeeropdracht, de hoofd- en deelvragen van het uit te voeren onderzoek en de op te leveren producten zoals hiervoor beschreven.
Bovendien verklaren zij dat op basis van deze gegevens door de student een plan van aanpak is geschreven dat door betrokkenen is goedgekeurd.

Handtekeningen

Datum :

Student :

Docentbegeleider :

Bedrijfsbegeleider[9] :

[9] **Door ondertekening van dit formulier verklaart de bedrijfsbegeleider (en eventuele mede-begeleiders) over voldoende kennis te beschikken, op minimaal HBO-niveau, om de afstudeerder te begeleiden.**

Bijlage E Voorlopige literatuurlijst

(An overview of the SSL or TLS handshake, 2014)

(Crawford, 2011)

(Ferrigni, 2003)

(Firewall.cx, sd)

(McKinley, 2003)

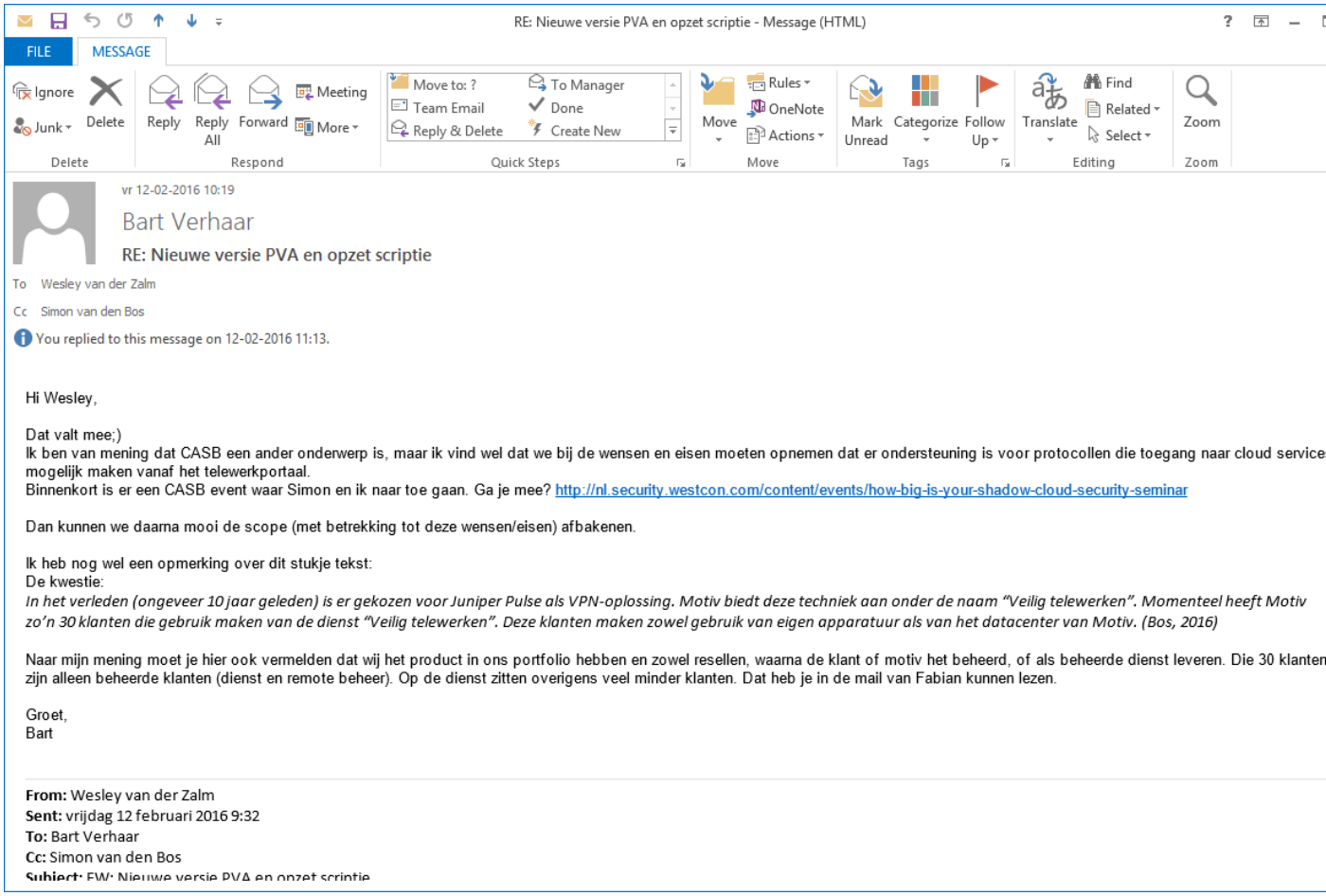
(OpenReach, 2002)

(Pillai, 2003)

(Sheila Frankel P. H., 2008)

(Govcert.nl, 2009)

Bijlage F Email Bart Verhaar



RE: Nieuwe versie PVA en opzet scriptie - Message (HTML)

FILE MESSAGE

Ignore Junk Delete | Reply Reply All Forward Meeting More | Move to: ? Team Email Reply & Delete To Manager Done Create New | Move Rules OneNote Actions | Mark Unread Categorize Follow Up | Translate Find Related Select | Zoom

Delete Respond Quick Steps Move Tags Editing Zoom

vr 12-02-2016 10:19

Bart Verhaar

RE: Nieuwe versie PVA en opzet scriptie

To Wesley van der Zalm

Cc Simon van den Bos

You replied to this message on 12-02-2016 11:13.

Hi Wesley,

Dat valt mee;)
Ik ben van mening dat CASB een ander onderwerp is, maar ik vind wel dat we bij de wensen en eisen moeten opnemen dat er ondersteuning is voor protocollen die toegang naar cloud service mogelijk maken vanaf het telewerkportaal.
Binnenkort is er een CASB event waar Simon en ik naar toe gaan. Ga je mee? http://nl.security.westcon.com/content/events/how-big-is-your-shadow-cloud-security-seminar

Dan kunnen we daarna mooi de scope (met betrekking tot deze wensen/eisen) afbakenen.

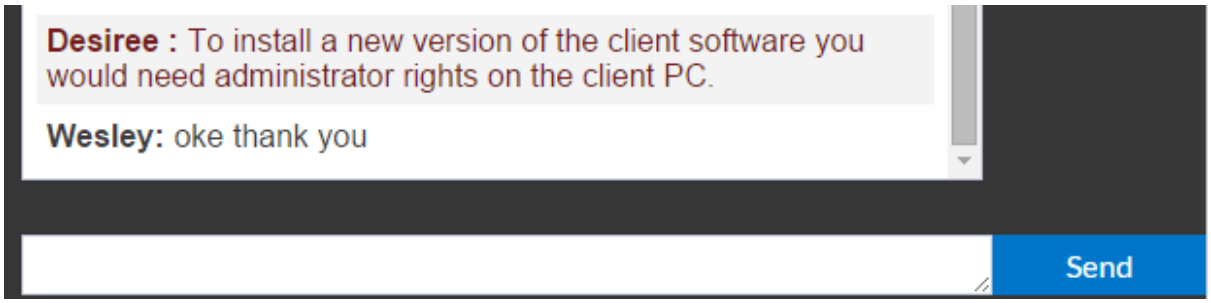
Ik heb nog wel een opmerking over dit stukje tekst:
De kwestie:
In het verleden (ongeveer 10 jaar geleden) is er gekozen voor Juniper Pulse als VPN-oplossing. Motiv biedt deze techniek aan onder de naam "Veilig telewerken". Momenteel heeft Motiv zo'n 30 klanten die gebruik maken van de dienst "Veilig telewerken". Deze klanten maken zowel gebruik van eigen apparatuur als van het datacenter van Motiv. (Bos, 2016)

Naar mijn mening moet je hier ook vermelden dat wij het product in ons portfolio hebben en zowel resellen, waarna de klant of motiv het beheerd, of als beheerde dienst leveren. Die 30 klanten zijn alleen beheerde klanten (dienst en remote beheer). Op de dienst zitten overigens veel minder klanten. Dat heb je in de mail van Fabian kunnen lezen.

Groet,
Bart

From: Wesley van der Zalm
Sent: vrijdag 12 februari 2016 9:32
To: Bart Verhaar
Cc: Simon van den Bos
Subject: FW: Nieuwe versie PVA en opzet scriptie

Bijlage 2 Contact met leveranciers



Figuur 14 Chat contact met Barracuda

vr 19-02-2016 08:31

Wesley van der Zalm

RE: [2016-02-18 21:25:37]英文站留言

Aan 'Jonathan - Sangfor'

Hi Jonathan,

I'm looking for a SSL VPN solution for our company which we can resell or deploy by our costumers (other enterprises).

So the solution need to be manageable. For example we implement one server which provide two or more costumers for an SSL VPN solution.

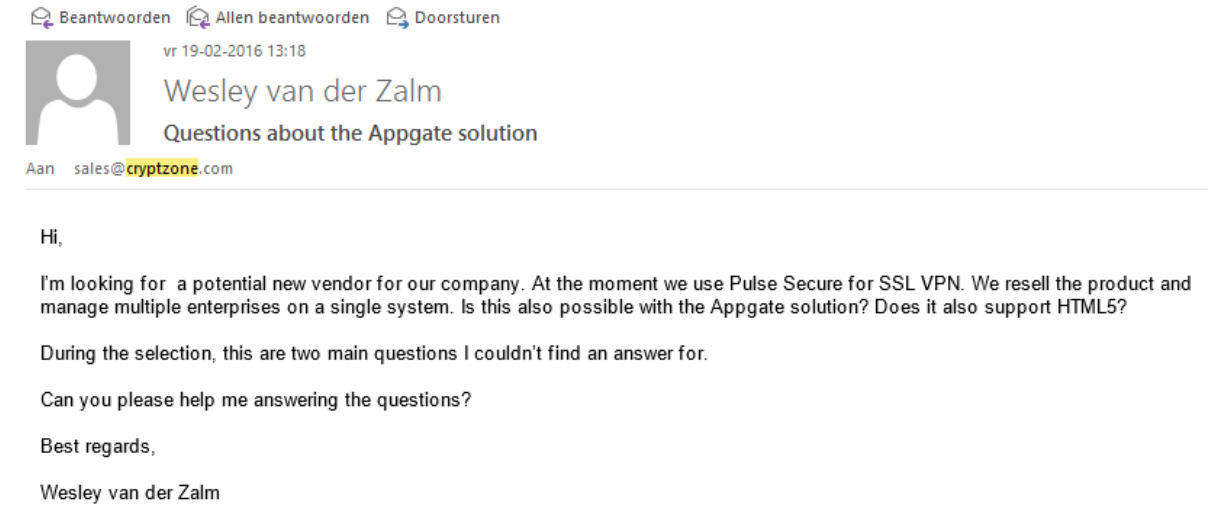
I have some other questions:

- Is there client software to provide access to virtual desktops?
- Which privileges does an Windows 7 user need to install it (administrator privileges)?
- And which privileges are required when there is an update for the software?
- Does the SSL VPN solution supports HTML5?

Thanks for helping me out.

Best regards,
Wesley van der Zalm

Figuur 15 Onbeantwoorde mail aan Sangfor



Beantwoorden Allen beantwoorden Doorsturen

vr 19-02-2016 13:18

Wesley van der Zalm

Questions about the Appgate solution

Aan sales@cryptzone.com

Hi,

I'm looking for a potential new vendor for our company. At the moment we use Pulse Secure for SSL VPN. We resell the product and manage multiple enterprises on a single system. Is this also possible with the Appgate solution? Does it also support HTML5?

During the selection, this are two main questions I couldn't find an answer for.

Can you please help me answering the questions?

Best regards,

Wesley van der Zalm

Figuur 16 Onbeantwoorde mail aan Cryptzone

Om concreet terug te komen op je vragen:

1) Is het mogelijk om bookmarks te definiëren (bijvoorbeeld een link naar intranet of webmail) die de gebruiker te zien krijgt na het inloggen op de portal (is het clientless te gebruiken)?
   - NetMotion is niet clientless te gebruiken. De client moet op het end-point geïnstalleerd worden. Dit kan via app/play store of via packages/MSI/etc. Omdat de client alles zelf automatisch regelt hoeft de gebruiker helemaal niets te doen.

2) Ondersteund de oplossing een multi-tenant architectuur?
   - De oplossing is niet gebouwd om multi-tenant te functioneren. Authenticatie moet plaatsvinden vanuit de DA van de organisatie, al dan niet in combinatie met 2FA. Het is wel mogelijk om de oplossing te hosted en delegated admin uit te voeren. Maar je zal dus per klantomgeving een aparte server moeten installeren voor die klant. Alles is wel virtueel te installeren en failover/redundancy zijn erg eenvoudig op te tuigen. NetMotion kan op een Windows Server geïnstalleerd worden, dus geen extra hoge kosten aan die kant zoals bij veel andere VPN oplossingen.

Met vriendelijke groet / With kind regards,

NetBoss
MANAGE YOUR (MOBILE) NETWORK

Stefan van Vlerken
NetBoss BV | Bennekomseweg 41 | 6717 LL | Ede | The Netherlands

Figuur 17 Antwoord van NetBoss

Bijlage 3 Voorbereiding interview en enquête

Voorbereiding interview

Voor het interview binnen Motiv zijn een aantal vragen ter voorbereiding opgesteld. Gedurende het interview verwacht ik dat er meer vragen naar boven komen. Er gaat een gesprek plaatsvinden waarbij Bart Verhaar, Simon van den Bos en Fabian Gugelot alle drie aanwezig zijn. Hier is bewust voor gekozen om meer interactie te krijgen gedurende het gesprek. Zelf denk ik zo het beste beeld te kunnen krijgen van de eisen en wensen.

Te stellen vragen:

- Moeten alle gegevens verwijderd worden als de sessie wordt beëindigd? Denk hierbij aan cache, cookies, opgeslagen wachtwoorden en URL's? Zowel op Windows, MAC, iOS en Android apparaten?
- Willen ze liever een op zich zelf staande appliance ipv firewall? Moet hier rekening worden gehouden met scores?
- Hoeveel licenties zijn er nodig? En hoeveel meer in de toekomst?
- Zijn er eisen voor support? Reactietijd en eventuele oplostijd?
- Is de aanpasbaarheid van de portal belangrijk?
- Moet er een mobiele pagina voor smartphones en tablets komen?
- Hoe belangrijk is een hoge beschikbaarheid? Moet het mogelijk zijn om failover clusters te maken en loadbalancing uit te voeren?
- Zijn er eisen/wensen met betrekking tot het back-uppen van het systeem?
- Zijn er verschillende rollen? Beheer, gebruikers, externe. Hoe is dit bij de klanten geregeld?
- Is het voor monitoring voldoende dat de oplossingen te koppelen zijn met ArcSight? Of zijn hier nog specifieke eisen voor?
- Welke beheertools moeten minimaal toegankelijk zijn? SSHv2/Telnet? Of Putty via RDP?
- Wat gaan er voor checks worden ingevoerd voor de hosts?
- Moet er gekeken worden naar IDS en IPS mogelijkheden van de oplossing?
- Zijn er vragen vanuit de geïnterviewde?
- Zijn er zaken die ik vergeten ben?

Voorbereiding enquête

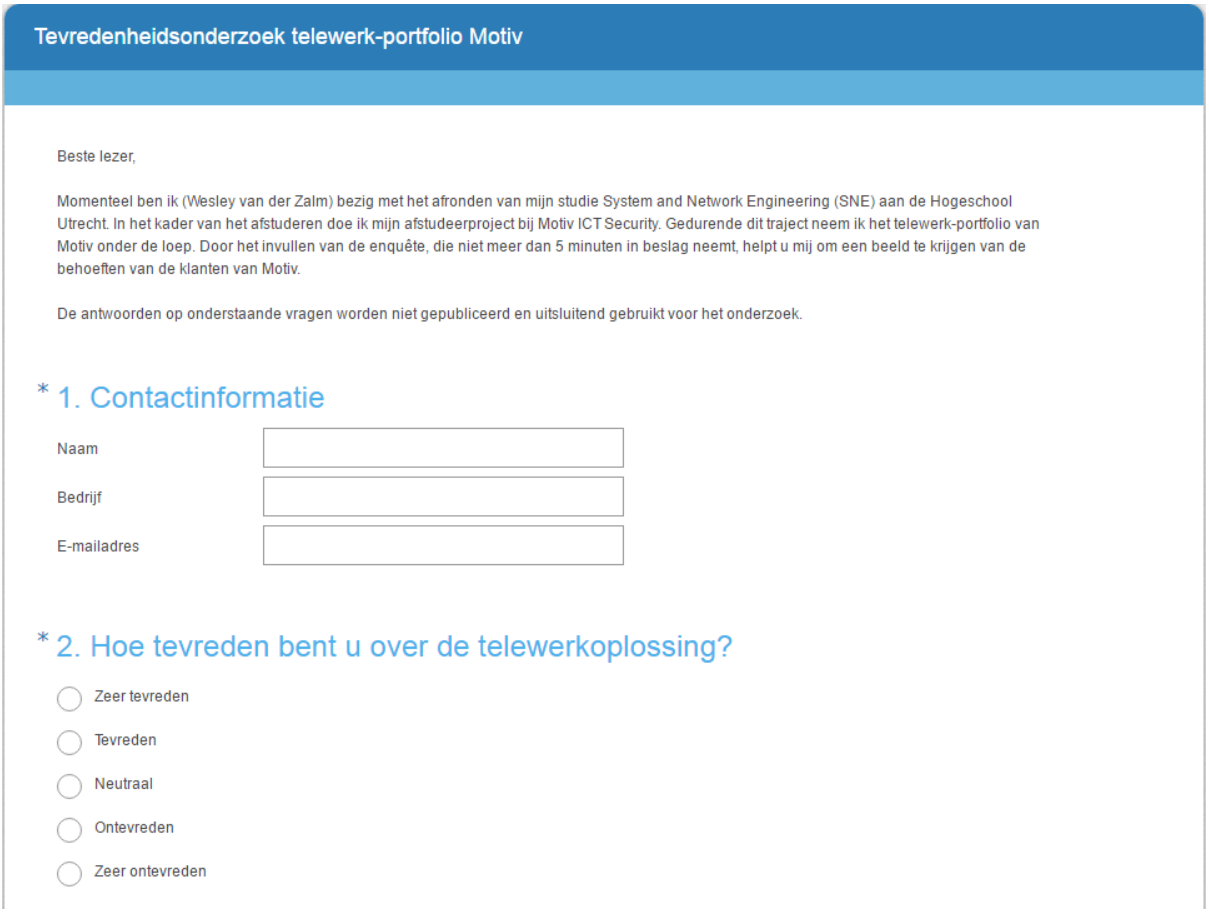
Naast het afnemen en verwerken van het interview, is het zaak om de klanten van Motiv een enquête in te laten vullen. Dit is nodig om de eisen en wensen van de klanten in beeld te krijgen. De medewerkers van Motiv (de geïnterviewde, Simon van den Bos, Bart Verhaar en Fabian Gugelot) zeggen de behoeften van de klanten te kennen. Om dit bevestigd te hebben en eventuele aanvullingen op eisen en wensen te krijgen, wordt de enquête afgenomen.

De enquête wordt verzonden naar de ICT-medewerkers van zes verschillende klanten. Sommige bedrijven nemen de gehele dienst 'Veilig Telewerken' af. Anderen hebben de oplossing zelf in beheer.

De klanten van Motiv die de enquête ontvangen zijn:

- Joanknecht
- Timeos
- Ruys
- Valuecare
- Kawasaki
- NBA

Hieronder vindt u de enquête zoals deze is verzonden aan de klanten van Motiv.



Tevredenheidsonderzoek telewerk-portfolio Motiv

Beste lezer,

Momenteel ben ik (Wesley van der Zalm) bezig met het afronden van mijn studie System and Network Engineering (SNE) aan de Hogeschool Utrecht. In het kader van het afstuderen doe ik mijn afstudeerproject bij Motiv ICT Security. Gedurende dit traject neem ik het telewerk-portfolio van Motiv onder de loep. Door het invullen van de enquête, die niet meer dan 5 minuten in beslag neemt, helpt u mij om een beeld te krijgen van de behoeften van de klanten van Motiv.

De antwoorden op onderstaande vragen worden niet gepubliceerd en uitsluitend gebruikt voor het onderzoek.

* 1. Contactinformatie

Naam

Bedrijf

E-mailadres

* 2. Hoe tevreden bent u over de telewerkoplossing?

Zeer tevreden

Tevreden

Neutraal

Ontevreden

Zeer ontevreden

* 3. Hoe belangrijk vindt u de volgende (technische) functionaliteiten?

	Uitermate belangrijk	Zeer belangrijk	Enigszins belangrijk	Niet erg belangrijk	Helemaal niet belangrijk
Telewerken zonder het installeren van software (clientless)	○	○	○	○	○
Mobiele weergave van de webpagina	○	○	○	○	○
Hoge beschikbaarheid	○	○	○	○	○
Toegangscontrole van de end-points (host-checking)	○	○	○	○	○
Eigen huisstijl van de portal	○	○	○	○	○
Ondersteuning van de nieuwste besturingssystemen (denk aan Windows 10)	○	○	○	○	○
Weergave van virtuele desktops binnen uw webbrowser (HTML5)	○	○	○	○	○

* 4. Zijn er (technische) functionaliteiten die u mist wanneer u gebruik maakt van de telewerkoplossing?

○ Nee

○ Ja, namelijk:

5. Kunt u per functionaliteit die u mist, aangeven hoe belangrijk dit is voor uw organisatie?

* 6. Zijn er andere zaken met betrekking tot de telewerkoplossing, die volgens u verbeterd kunnen worden?

○ Nee

○ Ja, namelijk:

Bijlage 4 Uitslagen enquête

V1: Contactinformatie

- **Naam**Johan Meijer
- **Bedrijf**Kawasaki Motors Europe
- **E-mailadres**j.meijer@kawasaki.eu

V2: Hoe tevreden bent u over de telewerkoplossing?

- Neutraal

V3: Hoe belangrijk vindt u de volgende (technische) functionaliteiten?

- **Telewerken zonder het installeren van software (clientless)**Zeer belangrijk
- **Mobiele weergave van de webpagina**Enigszins belangrijk
- **Hoge beschikbaarheid**Uitermate belangrijk
- **Toegangscontrole van de end-points (host-checking)**Zeer belangrijk
- **Eigen huisstijl van de portal**Enigszins belangrijk
- **Ondersteuning van de nieuwste besturingssystemen (denk aan Windows 10)**Zeer belangrijk
- **Weergave van virtuele desktops binnen uw webbrowser (HTML5)**Enigszins belangrijk

V4: Zijn er (technische) functionaliteiten die u mist wanneer u gebruik maakt van de telewerkoplossing?

- **Ja, namelijk:**Checkpoint VPN heeft locale admin rechten nodig bij updates. Hier willen we graag vanaf.

V5: Kunt u per functionaliteit die u mist, aangeven hoe belangrijk dit is voor uw organisatie?

Belangrijk: dit scheelt ons veel tijd bij de GPO installaties.

V6: Zijn er andere zaken met betrekking tot de telewerkoplossing, die volgens u verbeterd kunnen worden?

- **Ja, namelijk:**Meerdere portals in onze oplossing: voor klanten, leveranciers en eindgebruikers.

V1: Contactinformatie

- **Naam**Joost Kemps
- **Bedrijf**Joanknecht & Van Zelst
- **E-mailadres**jkemps@joanknecht.nl

V2: Hoe tevreden bent u over de telewerkoplossing?

- Tevreden

V3: Hoe belangrijk vindt u de volgende (technische) functionaliteiten?

- **Telewerken zonder het installeren van software (clientless)**Enigszins belangrijk
- **Mobiele weergave van de webpagina**Zeer belangrijk
- **Hoge beschikbaarheid**Zeer belangrijk
- **Toegangscontrole van de end-points (host-checking)**Zeer belangrijk
- **Eigen huisstijl van de portal**Niet erg belangrijk
- **Ondersteuning van de nieuwste besturingssystemen (denk aan Windows 10)**Zeer belangrijk
- **Weergave van virtuele desktops binnen uw webbrowser (HTML5)**Enigszins belangrijk

V4: Zijn er (technische) functionaliteiten die u mist wanneer u gebruik maakt van de telewerkoplossing?

- **Ja, namelijk:**Windows 10 ondersteuning!

V5: Kunt u per functionaliteit die u mist, aangeven hoe belangrijk dit is voor uw organisatie?

Zeer belangrijk

V6: Zijn er andere zaken met betrekking tot de telewerkoplossing, die volgens u verbeterd kunnen worden?

- Nee

V1: Contactinformatie

- **Naam**Walter Koper
- **Bedrijf**NBA
- **E-mailadres**w.koper@nba.nl

V2: Hoe tevreden bent u over de telewerkoplossing?

- Neutraal

V3: Hoe belangrijk vindt u de volgende (technische) functionaliteiten?

- **Telewerken zonder het installeren van software (clientless)**Uitermate belangrijk
- **Mobiele weergave van de webpagina**Zeer belangrijk
- **Hoge beschikbaarheid**Enigszins belangrijk
- **Toegangscontrole van de end-points (host-checking)**Enigszins belangrijk
- **Eigen huisstijl van de portal**Enigszins belangrijk
- **Ondersteuning van de nieuwste besturingssystemen (denk aan Windows 10)**Zeer belangrijk
- **Weergave van virtuele desktops binnen uw webbrowser (HTML5)**Zeer belangrijk

V4: Zijn er (technische) functionaliteiten die u mist wanneer u gebruik maakt van de telewerkoplossing?

- **Ja, namelijk:**functioneel niet, technisch wel: Het feit dat er geen Virtual versie is vind ik een groot gemist!

V5: Kunt u per functionaliteit die u mist, aangeven hoe belangrijk dit is voor uw organisatie?

een virtuele versie geeft de mogelijkheid deze op te nemen in BCP. Dan heb je tijdens een eventuele (gedeeltelijke) uitwijk geen last van hardware die nog moet komen en config settings die overgezet moeten worden.

V6: Zijn er andere zaken met betrekking tot de telewerkoplossing, die volgens u verbeterd kunnen worden?

- Nee

V1: Contactinformatie

- **Naam**Erik Radder
- **Bedrijf**FP-Ruys
- **E-mailadres**e.radder@fp-ruys.nl

V2: Hoe tevreden bent u over de telewerkoplossing?

- Tevreden

V3: Hoe belangrijk vindt u de volgende (technische) functionaliteiten?

- **Telewerken zonder het installeren van software (clientless)**Enigszins belangrijk
- **Mobiele weergave van de webpagina**Niet erg belangrijk
- **Hoge beschikbaarheid**Zeer belangrijk
- **Toegangscontrole van de end-points (host-checking)**Zeer belangrijk
- **Eigen huisstijl van de portal**Niet erg belangrijk
- **Ondersteuning van de nieuwste besturingssystemen (denk aan Windows 10)**Enigszins belangrijk
- **Weergave van virtuele desktops binnen uw webbrowser (HTML5)**Zeer belangrijk

V4: Zijn er (technische) functionaliteiten die u mist wanneer u gebruik maakt van de telewerkoplossing?

- Nee

V5: Kunt u per functionaliteit die u mist, aangeven hoe belangrijk dit is voor uw organisatie?

Respondent heeft deze vraag overgeslagen

V6: Zijn er andere zaken met betrekking tot de telewerkoplossing, die volgens u verbeterd kunnen worden?

- Nee

Ben ik tevreden over Telewerken: nee.

Belangrijke functionaliteit die we missen:

1. Kunnen werken met dubbele schermen
2. Mogelijkheid voor gebruikers zich (bv tijdens weekend) te kunnen unlocken (zodat ze niet gedwongen zijn tot maandag te wachten)
3. Mogelijkheid voor Mac gebruikers om van de dienst gebruik te maken zonder dat daar extra (dure) licenties voor nodig zijn, die nota bene alleen beschikbaar zijn in de staffel 2 of 50 gelijktijdige gebruikers.

Andere zaken die verbeterd kunnen worden:

(voor de eerste keer) ermee werken is niet gebruiksvriendelijk:

1. installatie Juniper is gefragmenteerd en onduidelijk
2. niet alle nieuwe versies van browserversies worden ondersteund
3. te hoge afhankelijkheid van Java
4. te vaak worden er geen sms-jes verstuurd, waardoor de dienst op dat moment onbruikbaar is

Met vriendelijke groet,

Guy Duijzings
Manager Supply Management
Supply Management

Bijlage 5 Bevestiging '*Key Criteria*'

di 03-05-2016 10:57

Bart Verhaar

RE: Key Criteria a.d.h.v. gesprek op 24-02-16

Aan Wesley van der Zalm

Akkoord

From: Wesley van der Zalm
Sent: dinsdag 3 mei 2016 8:33
To: Bart Verhaar
Subject: Key Criteria a.d.h.v. gesprek op 24-02-16

Key criteria	Reden
Radius, LDAP, SAML	Protocollen die nodig zijn voor de authenticatie van gebruikers.
Ondersteuning van minimaal de volgende besturingssystemen: Mac OSX, iOS, Android, Windows 7, Windows 8 en Windows 10.	Betreft de meest gebruikte Operating systemen van Motiv en klanten.
Multi-tenancy	Klanten moeten gescheiden beheerd kunnen worden.
Maximaal éénmalig lokale administratorrechten nodig voor het installeren van client-software.	Wanneer klanten bij elke update lokale administratorrechten nodig hebben, gaat dit voor veel gebruikersproblemen zorgen.
Minimaal ondersteuning voor: RDP, Citrix VDI (ICA) en VMware VDI (PCoIP)	Om virtuele machines via de VPN oplossing te kunnen benaderen. Een deel van de huidige klanten gebruikt hiervoor de Citrix oplossing en een ander deel de VMware oplossing. Beide typen virtuele desktops moeten dus ondersteund worden door een nieuwe oplossing.

Key Criteria	Reden
Bookmarks	Als gebruikers inloggen moeten ze bookmarks te zien krijgen, wanneer ze hier recht op hebben. Denk bijvoorbeeld aan fileshares (FTP), Terminal Services (RDP) via ActiveX of Java en voor beheerders aan SSH en Telnet.
VPN tunneling	Om veilig toegang te geven tot verschillende netwerk services.
Host-checker	Om devices van gebruikers eerst te kunnen controleren op bepaalde voorwaarden en aan de hand daarvan bepaalde resources te geven. Denk bijvoorbeeld aan up-to-date anti-virus software.
SNMP, Syslog en Koppeling HP ArcSight (SIEM)	SNMP en Syslog gegevens wordt naar de HP ArcSight SIEM oplossing gestuurd om de SSL VPN oplossing te kunnen monitoren.
Moet minimaal één van de volgende authenticatie-methode bevatten m.b.t. SSO: - Kerberos protocol - Basic authenticatie - NTLM protocol - Remote authenticatie	Door gebruik te maken van de Single Sign On techniek hoeven gebruikers maar één keer in te loggen. Deze techniek wordt in de huidige situatie in combinatie met sterke authenticatie al gebruikt en moet worden behouden.
Ondersteuning voor HTML5	Browsers die HTML5 ondersteunen bieden meer functionaliteit, zoals de opties om meer elementen te openen zonder plug-ins, het weergeven van video's en afspelen van audiofragmenten. Een SSL-VPN oplossing moet hier ook aan voldoen.
Er moet een mogelijkheid zijn om alleen SSL VPN te gebruiken (webbased en clientless)	Gebruikers moeten minimaal toegang hebben tot het bedrijfsnetwerk zonder software te hoeven installeren.

Bijlage 6 Testplan template

Testplan

De test wordt uitgevoerd in verschillende categorieën. De gebruikerstesten zullen uitgevoerd worden op een Windows 10 client machine.

Hostcheck

ID	Test
H1	Kan er gecontroleerd worden op Windows updates?
Uitslag	
Bewijs	

ID	Test
H2	Kan er gecontroleerd worden of er een antivirusprogramma aanwezig is?
Uitslag	
Bewijs	

ID	Test
H3	Kan er gecontroleerd worden wanneer een laatste virusscan is uitgevoerd?
Uitslag	
Bewijs	

ID	Test
H4	Kan er gecontroleerd worden of de client lid is van het domein?
Uitslag	
Bewijs	

ID	Test
H5	Kan er gecontroleerd worden welke processen er draaien?
Uitslag	
Bewijs	

ID	Test
H6	Kan de hostcheck elke half uur worden uitgevoerd?
Uitslag	
Bewijs	

Cache cleaning

ID	Test
C1	Kan de cache op de client worden verwijderd na een sessie?
Uitslag	
Bewijs	

ID	Test
C2	Kunnen cookies automatisch na een sessie worden verwijderd op de client?
Uitslag	
Bewijs	

ID	Test
C3	Kunnen opgeslagen wachtwoorden automatisch na een sessie worden verwijderd op de client?
Uitslag	
Bewijs	

ID	Test
C4	Kan cache automatisch na een sessie worden verwijderd op de server?
Uitslag	
Bewijs	

ID	Test
C5	Kunnen cookies automatisch na een sessie worden verwijderd op de server?
Uitslag	
Bewijs	

Technische functionaliteiten

ID	Test
T1	Kan er een logo worden weergegeven op de portal?
Uitslag	
Bewijs	

ID	Test
T2	Kan de achtergrond kleur worden aangepast van de portal?
Uitslag	
Bewijs	

ID	Test
T3	Kunnen er verschillende rollen per authenticatiemethode worden toegepast?
Uitslag	
Bewijs	

ID	Test
T4	Kunnen er verschillende rollen per gebruiker en per groep worden toegepast?
Uitslag	
Bewijs	

Gebruikerstest

ID	Test
G1	Is er een mobiele pagina voor gebruikers met een smartphone of tablet?
Uitslag	
Bewijs	

ID	Test
G2	Kan er gewerkt worden met meerdere monitoren?
Uitslag	
Bewijs	

ID	Test
G3	Is het mogelijk om een RDP sessie te starten vanaf de client?
Uitslag	
Bewijs	

ID	Test
G4	Is het eenvoudig om client software te installeren?
Uitslag	
Bewijs	

ID	Test
G5	Is het mogelijk om gebruik te maken van SSO (Single Sign-On)?
Uitslag	
Bewijs	

ID	Test
G6	Is het mogelijk om een RDP sessie binnen de browser te starten (HTML5)?
Uitslag	
Bewijs	

Score na test

Test	Score (0 t/m 10)	Weging (1 t/m 4)	Totaal
H1		3	
H2		3	
H3		3	
H4		3	
H5		3	
H6		3	
C1		4	
C2		4	
C3		4	
C4		4	
C5		4	
T1		4	
T2		4	
T3		4	
T4		4	
G1		3	
G2		4	
G3		4	
G4		4	
G5		4	
G6		4	
Totaal	-	-	

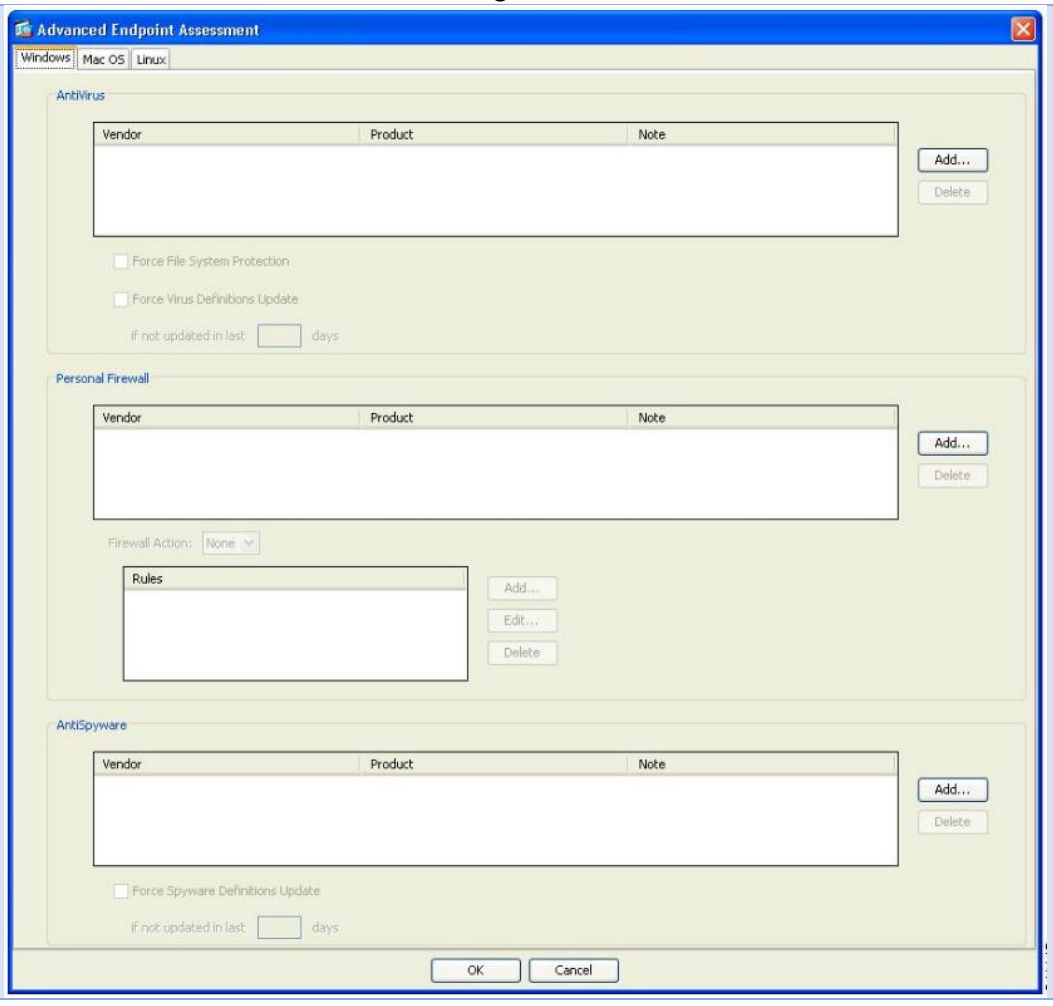
Bijlage 7 Testresultaten

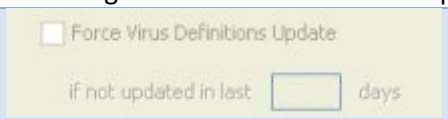
Cisco ASA

Hostcheck

Voor het testen van de Cisco ASA Hostscan is een plug-in nodig.

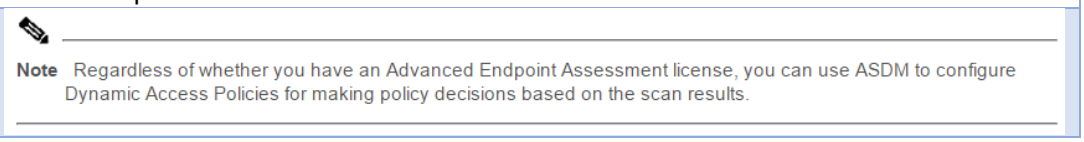
ID	Test
H1	Kan er gecontroleerd worden op Windows updates?
Uitslag	Nee. Hier is geen optie voor binnen de Hostscan.
Bewijs	http://www.cisco.com/c/en/us/td/docs/security/csd/csd34/configuration/guide/csd34cfg/CSDhscan.html

ID	Test
H2	Kan er gecontroleerd worden of er een antivirusprogramma aanwezig is?
Uitslag	Volgens de documentatie is dit mogelijk. Echter zijn hier plug-ins voor nodig waar ik niet over beschik. Hierdoor heb ik de aanwezigheid zelf niet kunnen testen.
Bewijs	

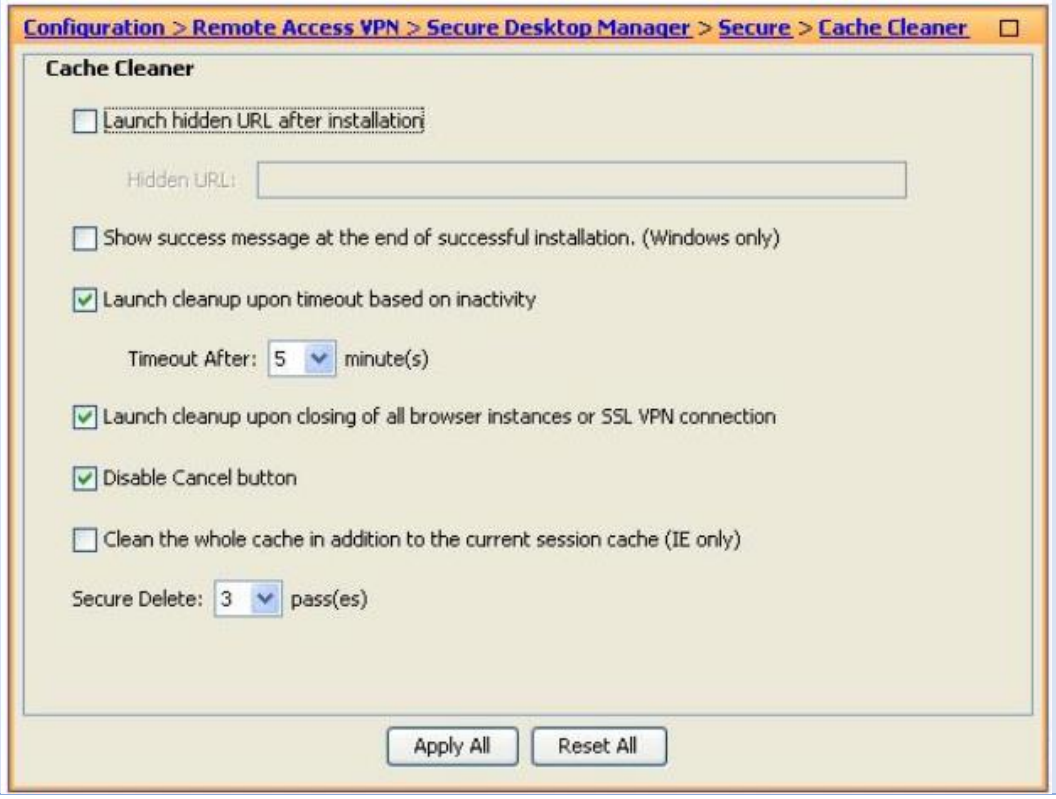
ID	Test
H3	Kan er gecontroleerd worden wanneer een laatste virusscan is uitgevoerd?
Uitslag	Niet kunnen testen, maar in de documentatie valt te lezen dat er alleen op aanwezigheid van een antivirus en updates daarvan gecontroleerd kan worden.
Bewijs	 http://www.cisco.com/c/en/us/td/docs/security/csd/csd34/configuration/guide/csd34cfg/CSDhscan.html

ID	Test
H4	Kan er gecontroleerd worden of de client lid is van het domein?
Uitslag	Volgens de documentatie is dit mogelijk. Echter zijn hier plug-ins voor nodig waar ik niet over beschik. Volgens onderstaande bron kan er gecontroleerd worden op registry keys. In het geval van een Windows 8 machine kan er gecontroleerd worden op de value van HKEY_CURRENT_USER\Volatile Envirionment\USERDNSDOMAIN.
Bewijs	http://www.cisco.com/c/en/us/td/docs/security/csd/csd34/configuration/guide/csd34cfg/CSDhscan.html

ID	Test
H5	Kan er gecontroleerd worden welke processen er draaien?
Uitslag	Volgens de documentatie is dit mogelijk. Echter zijn hier plug-ins voor nodig waar ik niet over beschik. Hierdoor heb ik zelf niet kunnen testen.
Bewijs	

ID	
H6	Kan de host-check elke half uur worden uitgevoerd?
Uitslag	Volgens de documentatie wordt de scan alleen uitgevoerd voordat een gebruiker in kan loggen. Op basis van de credentials en de uitslag van de Hostscan worden dynamische rechten bepaald.
Bewijs	

Cache cleaning

ID	Test
C1	Kan de cache op de client worden verwijderd na een sessie?
Uitslag	Volgens de documentatie is dit mogelijk. Helaas heb ik dit niet kunnen testen omdat ik niet beschik over de benodigde plug-ins.
Bewijs	

ID	Test
C2	Kunnen cookies automatisch na een sessie worden verwijderd op de client?
Uitslag	Cisco Secure Desktop biedt de mogelijkheid om overbodige cookies te verwijderen. Dit is helaas niet getest, omdat de benodigde plug-ins ontbreken.
Bewijs	http://www.cisco.com/c/en/us/td/docs/security/csd/csd311/csd_for_asa/configuration/311j/CSDJntro.html

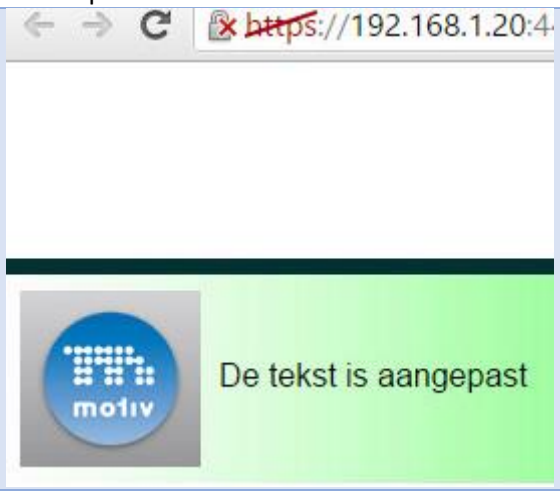
ID	Test
C3	Kunnen opgeslagen wachtwoorden automatisch na een sessie worden verwijderd op de client?
Uitslag	Volgens documentatie is dit mogelijk. Helaas is dit niet getest wegens het missen van plug-ins.
Bewijs	http://www.cisco.com/c/en/us/td/docs/security/csd/csd34/configuration/guide/csd34cfg/CSDsdcc.html

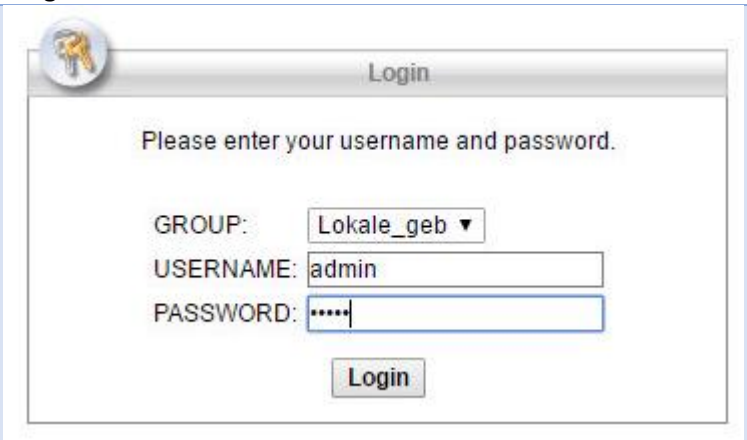
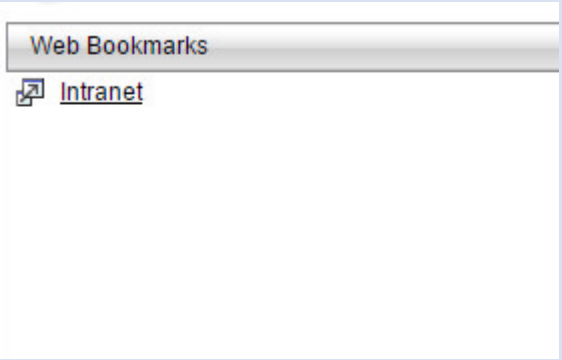
ID	Test
C4	Kan cache automatisch na een sessie worden verwijderd op de server?
Uitslag	Wegens ontbrekende plug-ins is dit niet getest. In de eerder genoemde documenten die betrekking hebben op de Cache Cleaner en de Secure Desktop Manager is er niets gevonden over het verwijderen van cache op de Cisco ASA.
Bewijs	N.V.T.

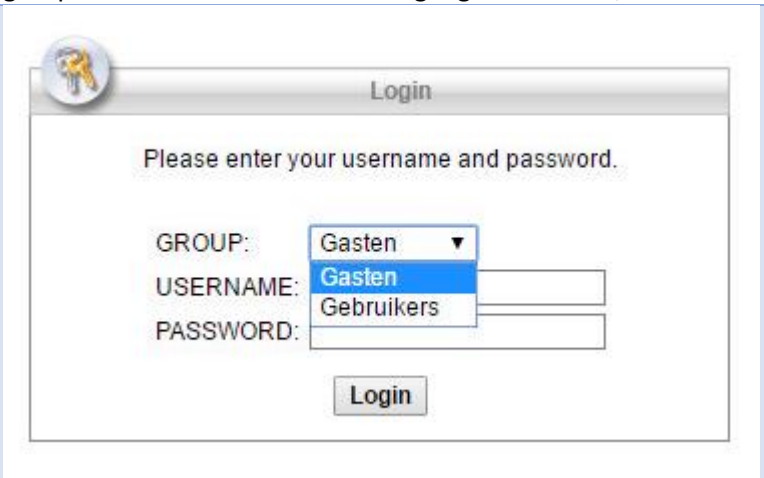
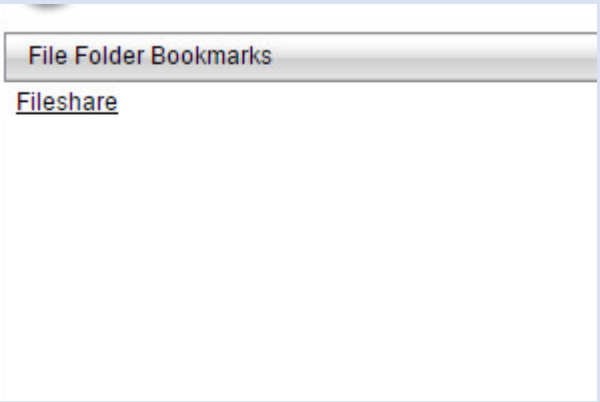
ID	Test
C5	Kunnen cookies automatisch na een sessie worden verwijderd op de server?
Uitslag	Wegens ontbrekende plug-ins is dit niet getest. In de eerder genoemde documenten die betrekking hebben op de Cache Cleaner en de Secure Desktop Manager is er niets gevonden over het verwijderen van cookies op de Cisco ASA.
Bewijs	N.V.T.

Technische functionaliteiten

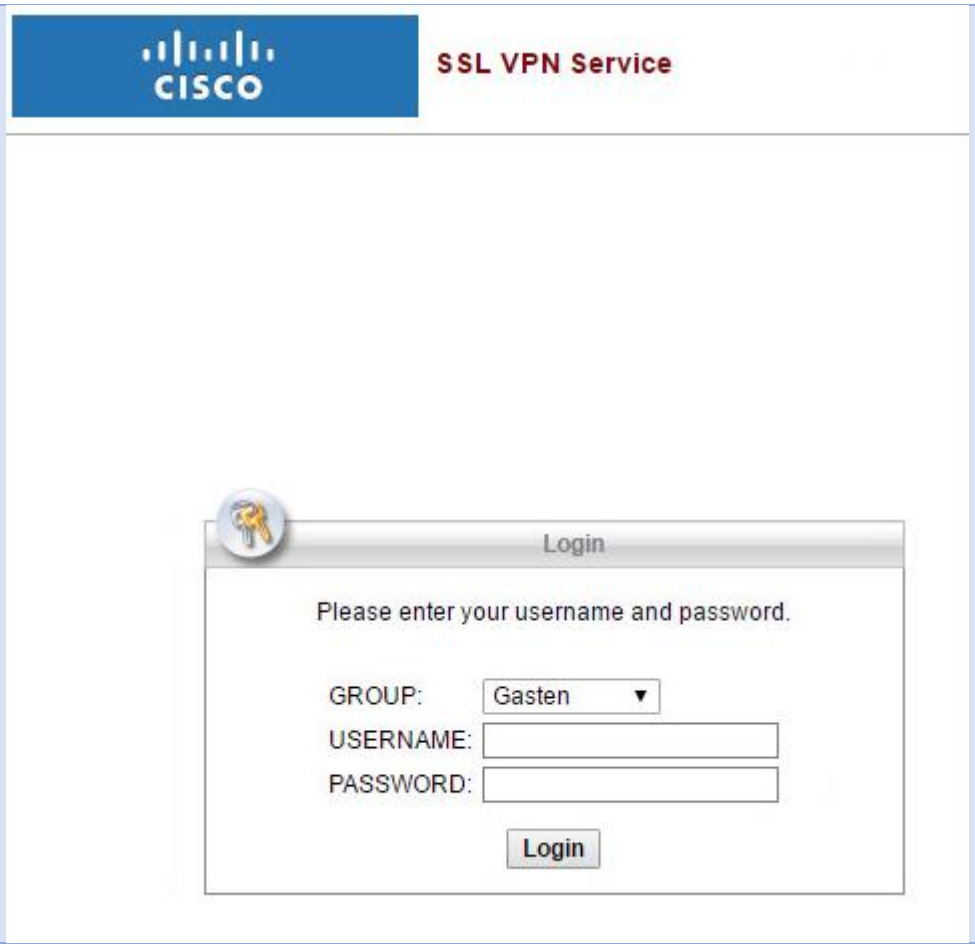
ID	Test
T1	Kan er een logo worden weergegeven op de portal?
Uitslag	Ja, deze kan eenvoudig via ASDM worden toegevoegd.
Bewijs	

ID	Test
T2	Kan de achtergrond kleur worden aangepast van de portal?
Uitslag	Ja de kleur is groen gemaakt om dit duidelijk te weergeven. Ook is de tekst eenvoudig aan te passen.
Bewijs	

ID	Test
T3	Kunnen er verschillende rollen per authenticatiemethode worden toegepast?
Uitslag	Om dit te testen is de groep ‘Lokale_geb’ aangemaakt. De authenticatiemethode is niet gekoppeld aan active directory, maar aan de lokale database op de Cisco ASA. Alleen een bookmark voor de intranetpagina is toegekend. Per authenticatiemethode kan er dus een groep worden aangemaakt. Aan de verschillende groepen kunnen rechten worden toegekend.
Bewijs	  

ID	Test
T4	Kunnen er verschillende rollen per gebruiker en per groep worden toegepast?
Uitslag	Om dit te testen zijn er twee groepen aangemaakt (Gasten en Gebruikers). Per groep kunnen bookmarks worden toegekend. Hieronder in de eerste afbeelding is te zien dat de twee groepen beschikbaar zijn. In de tweede afbeelding ben ik ingelogd als 'Gast' en heb ik alleen toegang tot een Fileshare. In de laatste afbeelding ben ik ingelogd onder de groep 'Gebruikers'. Deze heeft toegang tot intranet, de Fileshare en Remote Desktop.
Bewijs	  

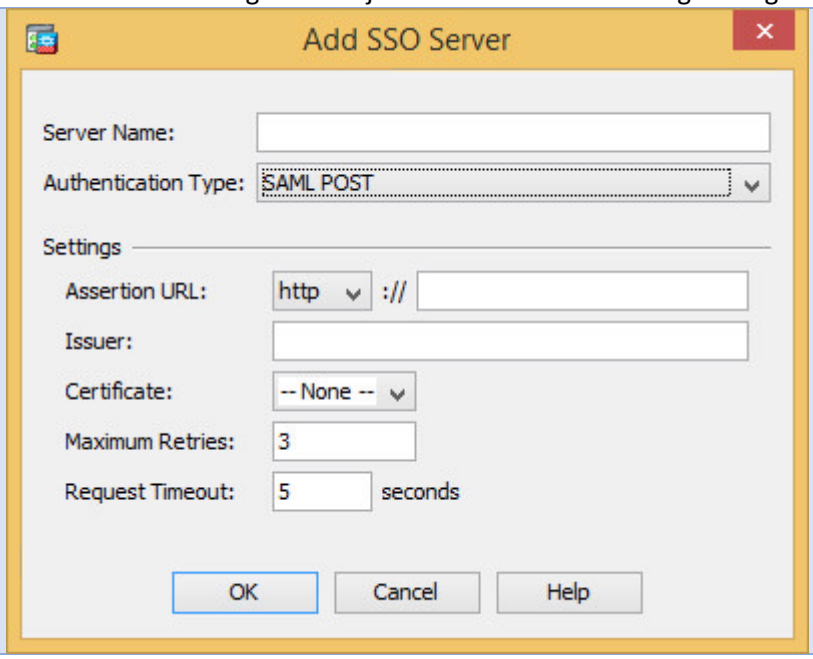
Gebruikerstest

ID	Test
G1	Is er een mobiele pagina voor gebruikers met een smartphone of tablet?
Uitslag	De pagina van de Cisco ASA kan worden weergegeven op de iPhone 6, iPad en Android. Echter is het geen mobiele pagina en moet er veel gescrold worden om er gebruik van te kunnen maken.
Bewijs	

ID	Test
G2	Kan er gewerkt worden met meerdere monitoren?
Uitslag	Dit heb ik niet kunnen testen omdat er plug-ins nodig zijn.
Bewijs	N.v.t.

ID	Test
G3	Is het mogelijk om een RDP sessie te starten vanaf de client?
Uitslag	Voor het starten van een RDP sessie is er een Java plug-in nodig. Op het internet heb ik er één gevonden, echter lijkt deze niet goed te werken. Het testen van RDP is gedaan op twee verschillende client machines (Windows 8 en Windows 10). Beide clients beschikken over de nieuwste Java versie. Ook is er in verschillende browsers getest (Firefox, Google Chrome en Internet Explorer). Alle webbrowsers geven hetzelfde resultaat, namelijk een zwart scherm.
Bewijs	

ID	Test
G4	Is het eenvoudig om client software te installeren?
Uitslag	Dit heb ik niet kunnen testen omdat er plug-ins nodig zijn.
Bewijs	NVT

ID	Test
G5	Is het mogelijk om gebruik te maken van SSO (Single Sign-On)
Uitslag	Ja. via ASDM kan er gemakkelijk een SSO server worden geconfigureerd.
Bewijs	

ID	Test
G6	Is het mogelijk om een RDP sessie binnen de browser te starten (HTML5)?
Uitslag	Dit zou mogelijk moeten zijn met gebruik van Java. Zoals te zien is bij G3 levert dit problemen op.
Bewijs	Zie G3

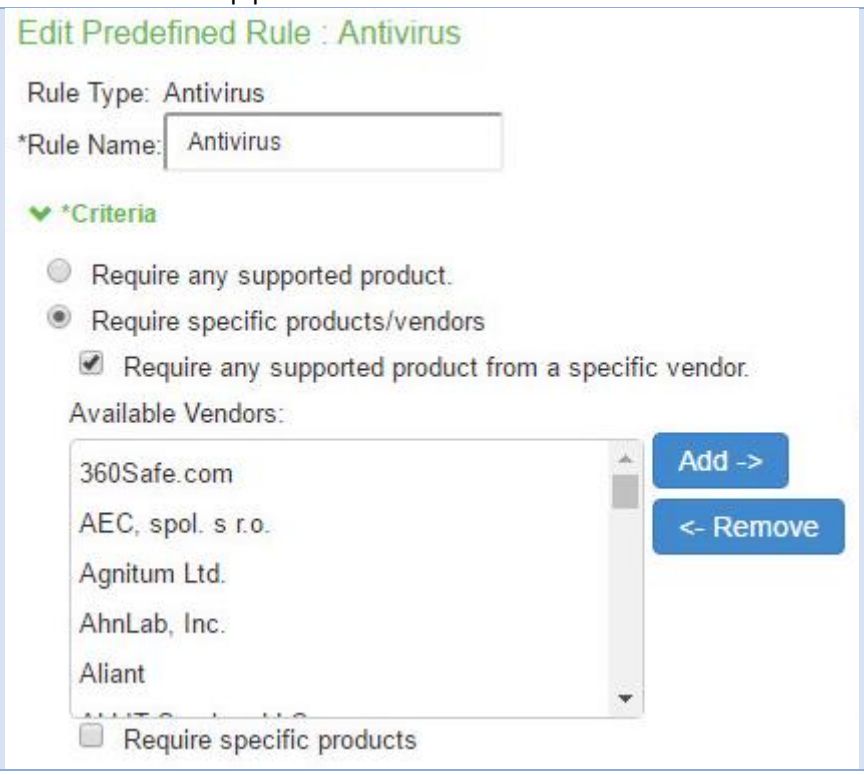
Score na test

Test	Score (0 t/m 10)	Weging (1 t/m 4)	Totaal
H1	0	3	0
H2	6	3	18
H3	8	3	24
H4	10	3	30
H5	10	3	30
H6	0	3	0
C1	8	4	32
C2	8	4	32
C3	8	4	32
C4	0	4	0
C5	0	4	0
T1	10	4	40
T2	10	4	40
T3	10	4	40
T4	10	4	40
G1	5	3	15
G2	0	4	0
G3	5	4	20
G4	0	4	0
G5	8	4	32
G6	5	4	20
Totaal	-	-	**445**

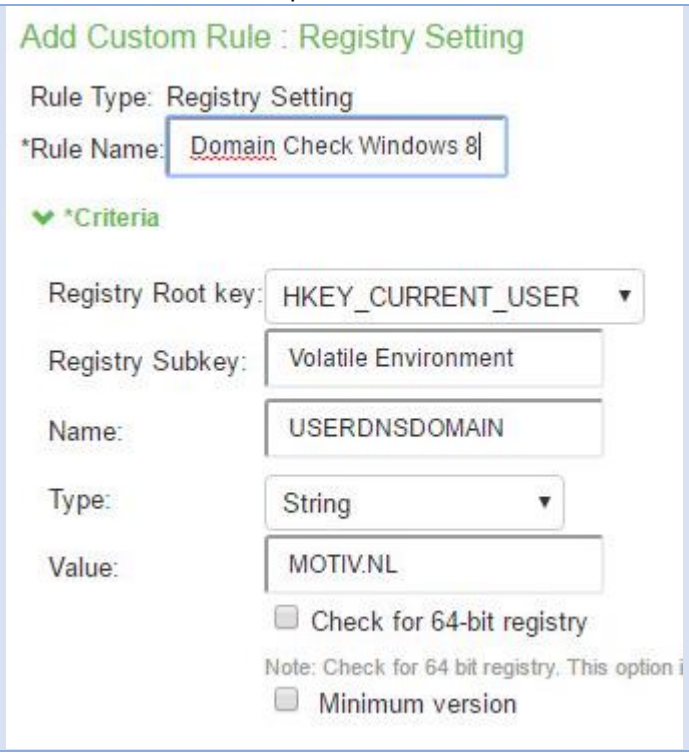
Pulse Secure

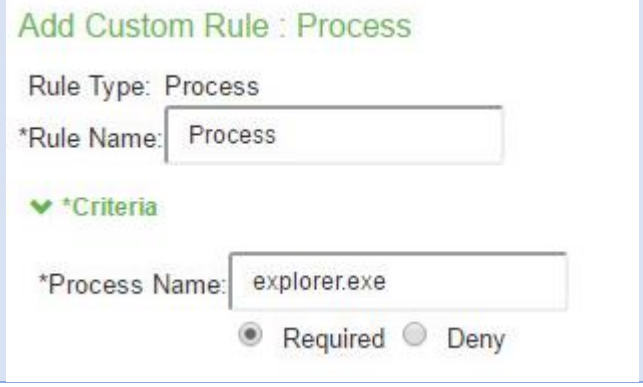
Hostcheck

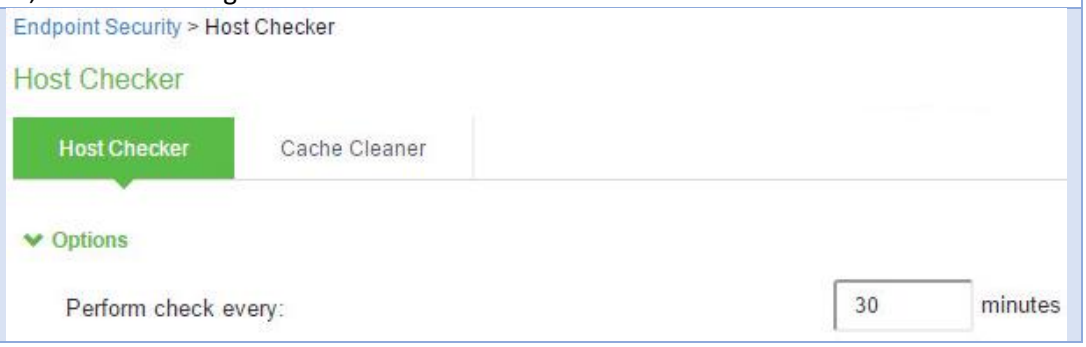
ID	Test
H1	Kan er gecontroleerd worden op Windows updates?
Uitslag	Nee. Wel is het mogelijk om te selecteren welke Windows versie of servicepack er nodig is om toegang te verlenen. Er is ruime keuze voor versies zoals Windows Server 2008/2012 en Client versies van Windows XP t/m Windows 10.
Bewijs	

ID	Test
H2	Kan er gecontroleerd worden of er een antivirusprogramma aanwezig is?
Uitslag	Ja, er is een regel aan te maken waar de beheerder kan bepalen, welke antivirussoftware aanwezig is op een clientsysteem. Hierbij kan gekeken worden op vendor niveau of op productniveau.
Bewijs	

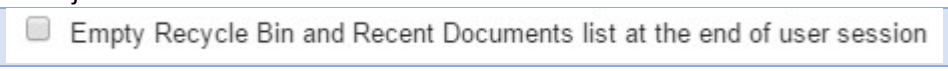
ID	Test
H3	Kan er gecontroleerd worden wanneer een laatste virusscan is uitgevoerd?
Uitslag	Ja, tijdens het maken van de regel die in H2 is beschreven, staat onderaan de optie om een eis te stellen wanneer de laatste scan moet zijn uitgevoerd.
Bewijs	

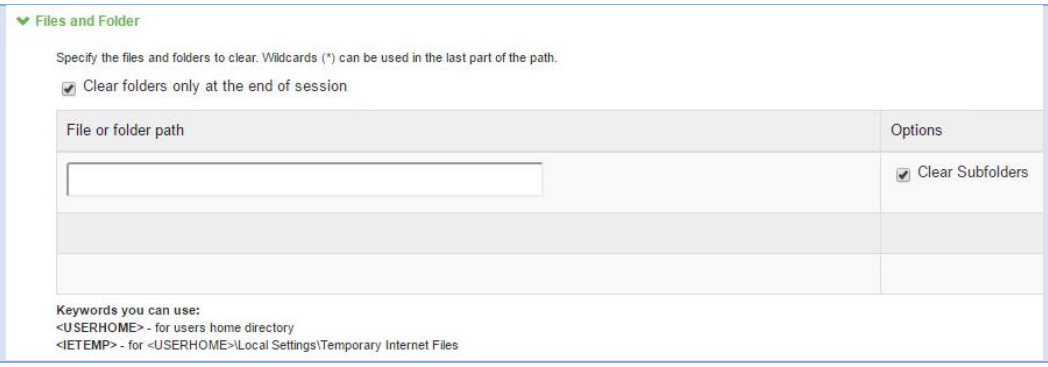
ID	Test
H4	Kan er gecontroleerd worden of de client lid is van het domein?
Uitslag	Hiervoor is geen predefined rule in Pulse Secure. Echter is het mogelijk om bijvoorbeeld op een Windows 8 machine te zoeken naar de registry key HKEY_CURRENT_USER\Volatile Envirionment\USERDNSDOMAIN. De value daarvan bevat in Windows 8 het domein. Echter geldt voor verouderde Windows versies zoals Windows XP een ander pad.
Bewijs	

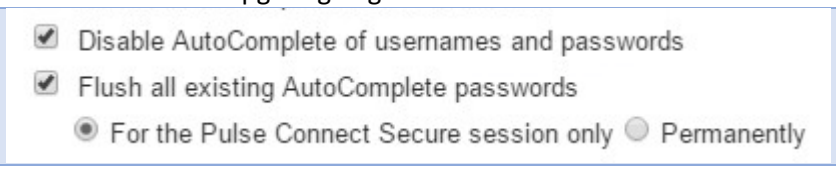
ID	Test
H5	Kan er gecontroleerd worden welke processen er draaien?
Uitslag	Het is mogelijk om processen te controleren, voordat er toegang wordt gegeven aan een machine. We kunnen kiezen of een proces wel of niet gestart moet zijn.
Bewijs	

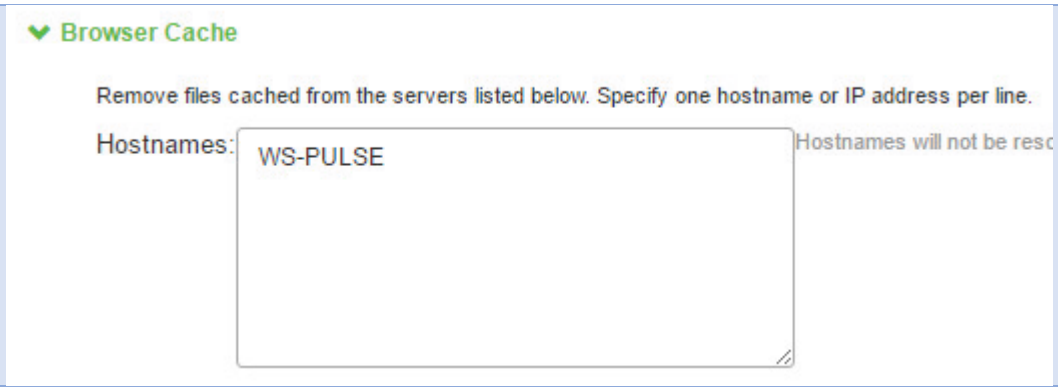
ID	Test
H6	Kan de host-check elke half uur worden uitgevoerd?
Uitslag	Ja, er kan worden gekozen hoe snel de host-check zich herhaalt.
Bewijs	

Cache cleaning

ID	Test
C1	Kan de cache op de client worden verwijderd na een sessie?
Uitslag	Ja, onder ‘Cache Cleaner’ is de onderstaande optie te vinden. Wanneer een gebruiker bijvoorbeeld vanaf een kiosk pc inlogt, is het mogelijk om alle gegevens na een sessie te verwijderen.
Bewijs	

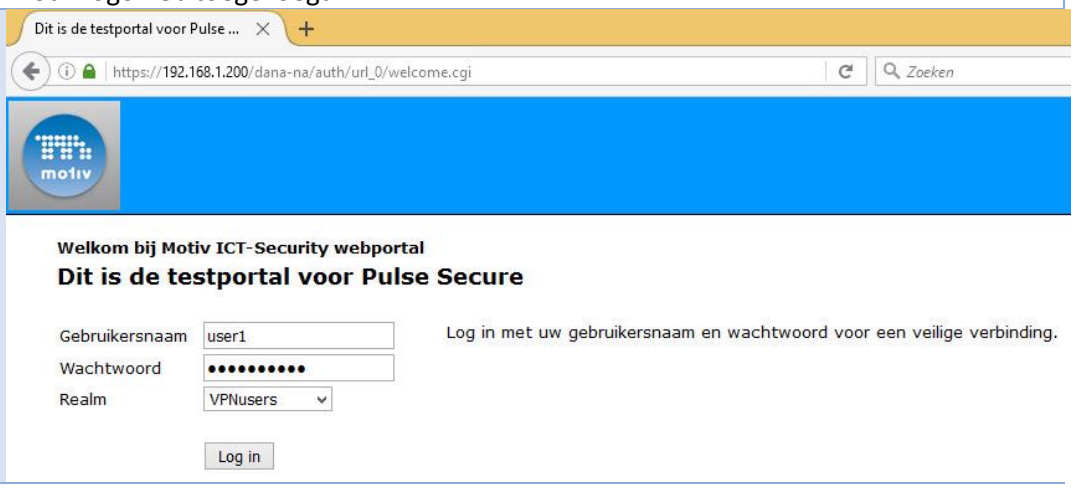
ID	Test
C2	Kunnen cookies automatisch na een sessie worden verwijderd op de client?
Uitslag	Het is mogelijk om alle cookies te verwijderen van de client. Dit kan door specifiek folders in te stellen die leeg gemaakt worden na een sessie. Echter wordt dit sterk afgeraden omdat de ‘Cache Cleaner’ gebruik maakt van een cookie genaamd ‘DSPREAUTH’. Wanneer deze verwijderd wordt, zal de ‘Cache Cleaner’ niet meer na behoren werken.
Bewijs	

ID	Test
C3	Kunnen opgeslagen wachtwoorden automatisch na een sessie worden verwijderd op de client?
Uitslag	Ja, reeds opgeslagen wachtwoorden voor een Pulse Secure sessie kunnen worden verwijderd. Er kan ook gekozen worden om AutoComplete uit te schakelen. Dit betekent echter niet dat de opgeslagen gebruikersnamen en wachtwoorden worden verwijderd.
Bewijs	

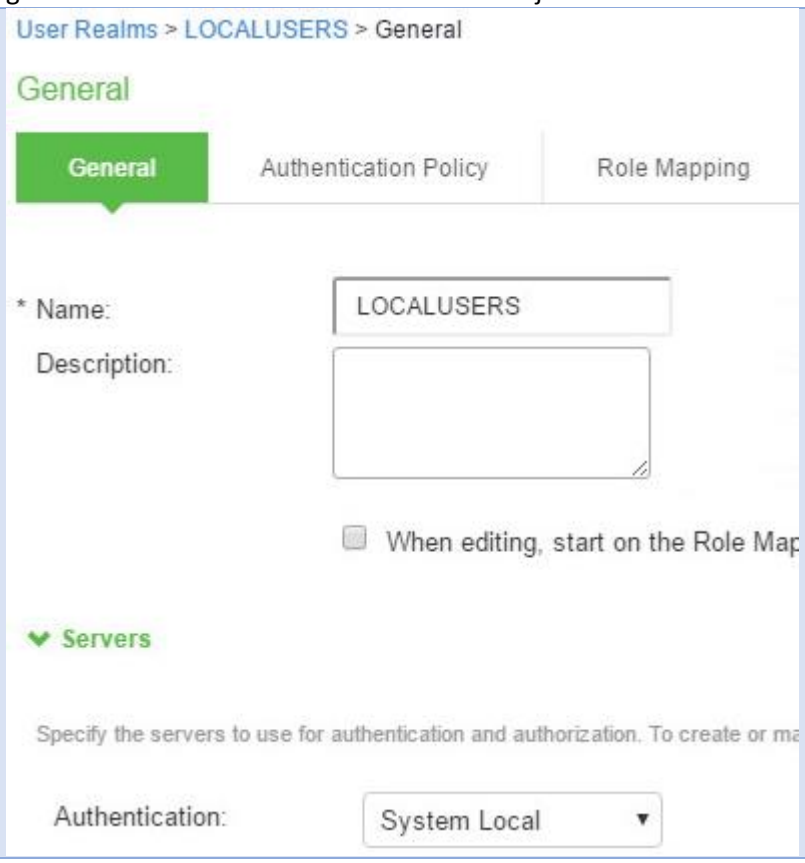
ID	Test
C4	Kan cache automatisch na een sessie worden verwijderd op de server?
Uitslag	Ja, een optie is om de hostname van de server op te geven. Na een sessie (of bij een aangegeven tijdsinterval) wordt in dit voorbeeld de cache verwijderd van de server WS-PULSE.
Bewijs	

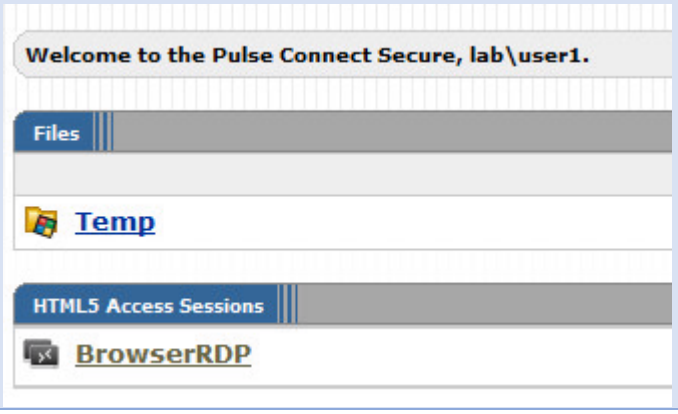
ID	Test
C5	Kunnen cookies automatisch na een sessie worden verwijderd op de server?
Uitslag	Cookies zijn ook gecached files. Zoals te zien is bij C4 is dit dus mogelijk.
Bewijs	Zie C4.

Technische functionaliteiten

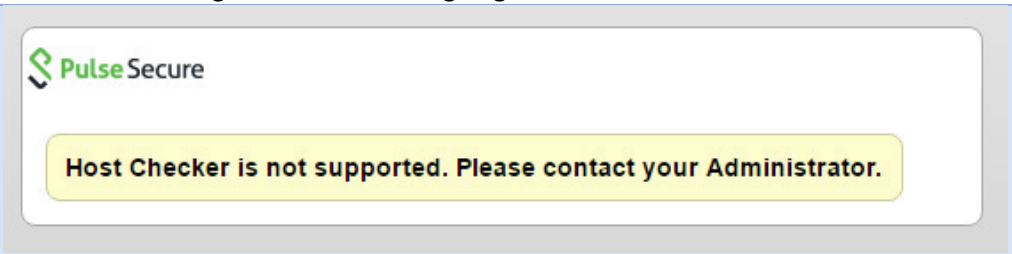
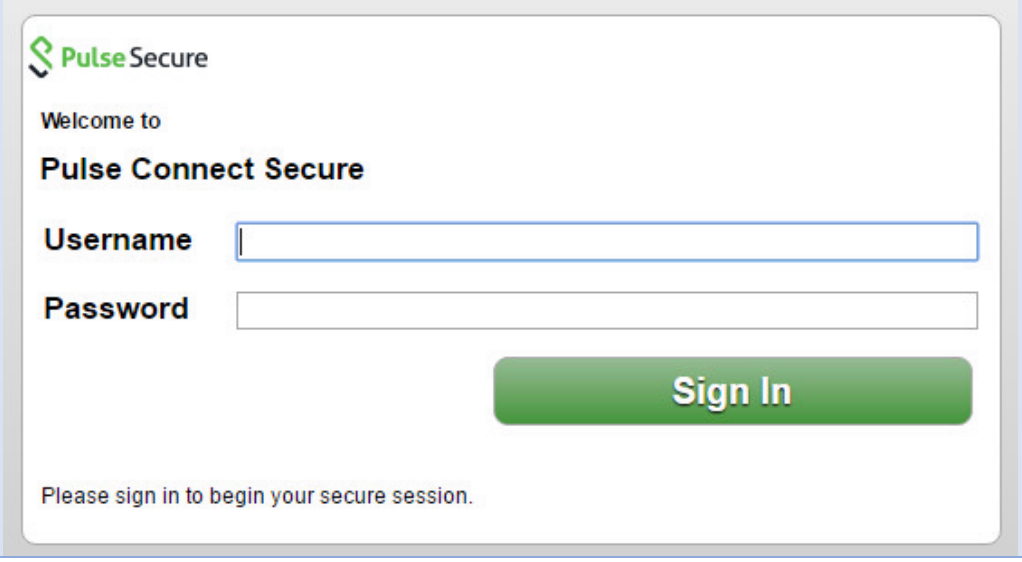
ID	Test
T1	Kan er een logo worden weergegeven op de portal?
Uitslag	Het logo van de portal is aanpasbaar. In onderstaande voorbeeld is te zien dat ik het Motiv logo heb toegevoegd.
Bewijs	

ID	Test
T2	Kan de achtergrond kleur worden aangepast van de portal?
Uitslag	Gedeeltelijk. Zoals te zien is, is alleen de bovenste balk (het verlengde van het logo) veranderd. De teksten en de melding die de Pulse Secure genereerd zijn eenvoudig te wijzigen.
Bewijs	

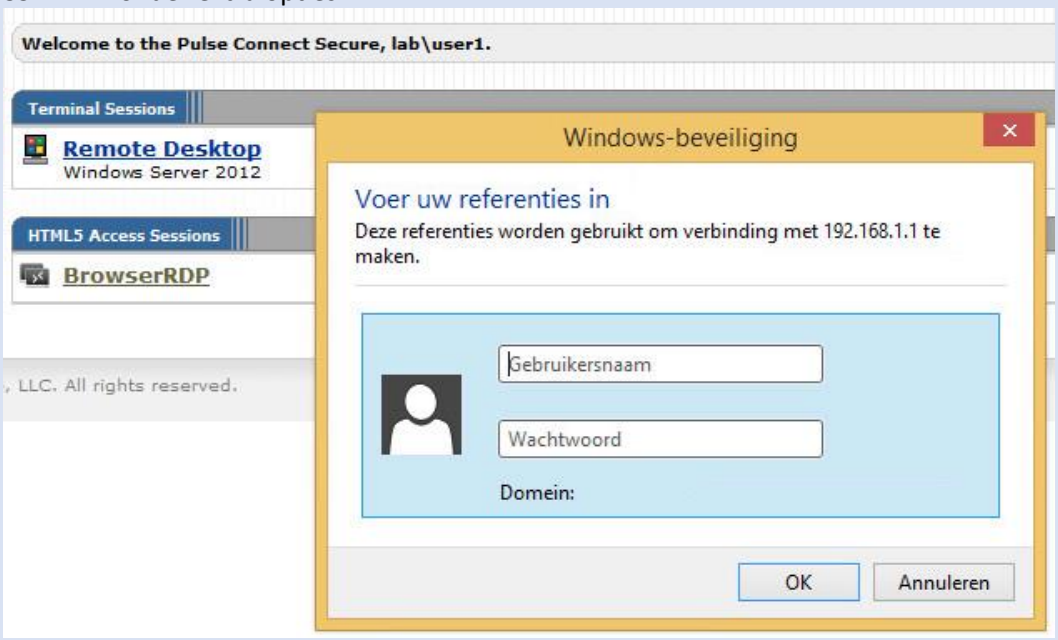
ID	Test
T3	Kunnen er verschillende rollen per authenticatiemethode worden toegepast?
Uitslag	Ja, er kunnen verschillende rollen per groep worden toegekend. Per groep is ook aan te geven wat de authenticatiemethode moet zijn.
Bewijs	

ID	Test
T4	Kunnen er verschillende rollen per gebruiker en per groep worden toegepast?
Uitslag	Ja, dit is getest met een AD gebruiker. Deze gebruiker (user1) is lid gemaakt van twee groepen (VPNusers en RDPVPNusers). Bij het inloggen wordt de keuze gesteld voor een groep. In het bewijs ziet u dat verschillende bookmarks zijn toegekend per groep. Wanneer ik een user2 aan zou maken en deze lid zou maken van een groep, krijgt de betreffende gebruiker dezelfde bookmarks.
Bewijs	 

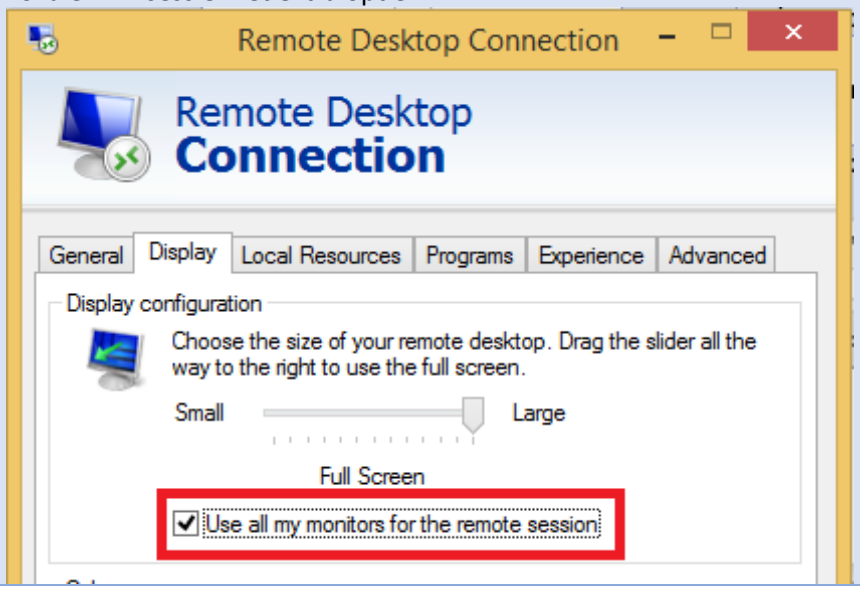
Gebruikerstest

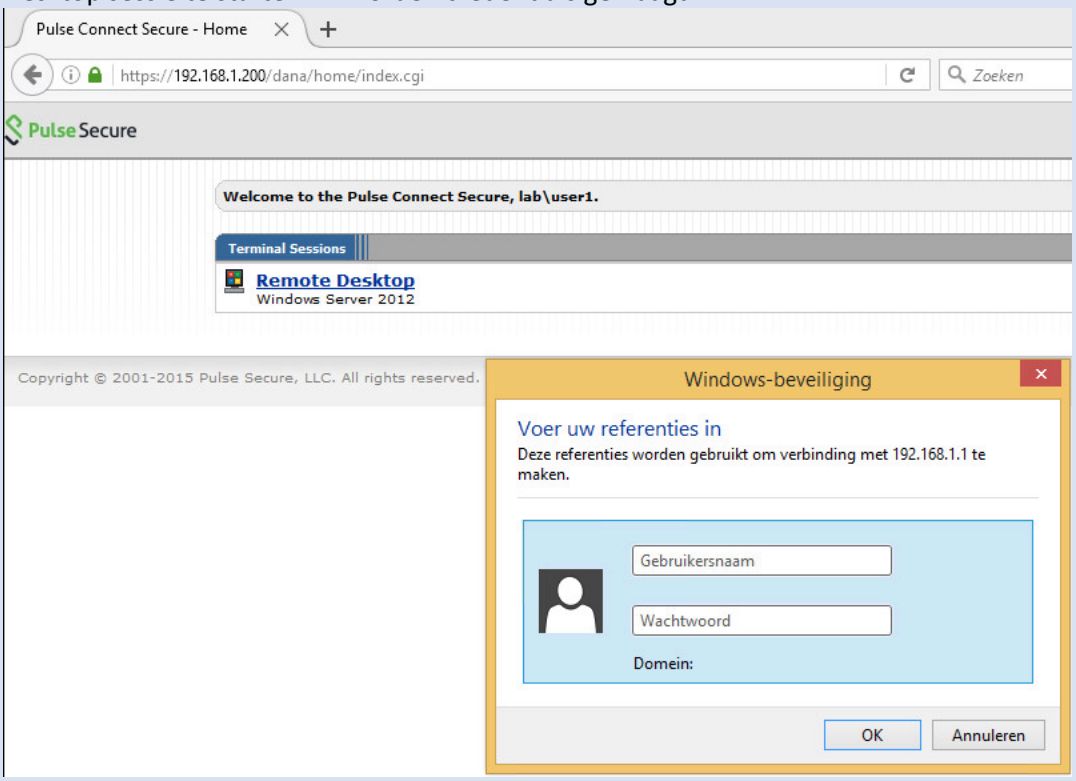
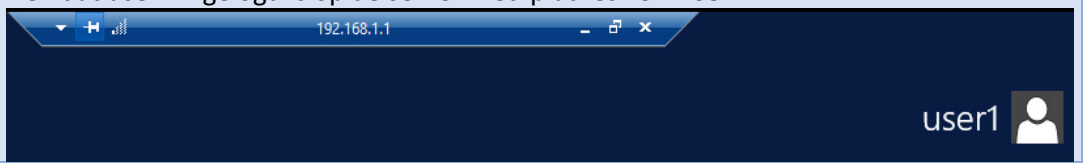
ID	Test
G1	Is er een mobiele pagina voor gebruikers met een smartphone of tablet?
Uitslag	Ja. Direct valt op dat bij een eerste test een melding verschijnt waarin staat dat de Host Checker niet uitgevoerd kan worden. Hiervoor is een aparte policy toegevoegd. In de tweede afbeelding is te zien dat er ingelogd kan worden via de mobiele site.
Bewijs	 

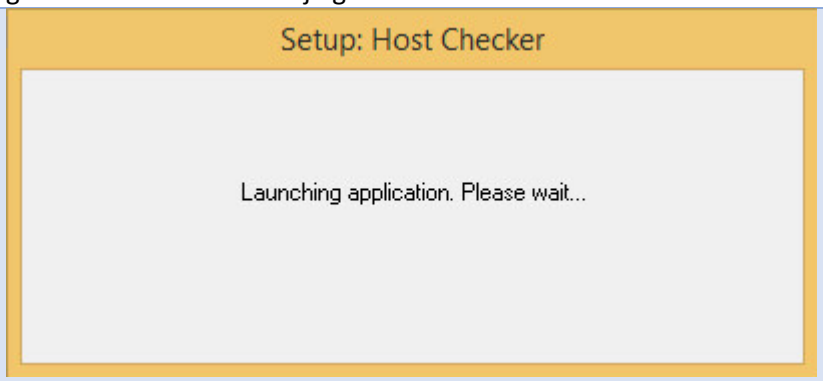
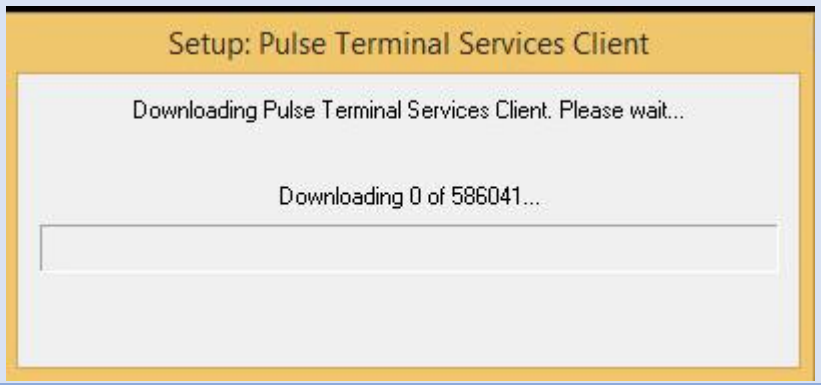
ID	Test
G2	Kan er gewerkt worden met meerdere monitoren?
Uitslag	Dit kan niet via RDP. Wanneer een RDP sessie wordt gestart binnen een netwerk, zijn er opties beschikbaar waar kan worden aangegeven dat alle monitoren gebruikt moeten worden. Via SSL VPN zijn deze opties er niet. Ook via HTML5 RDP is het niet mogelijk om met meerdere monitoren te worden.
Bewijs	SSL VPN zonder extra opties.

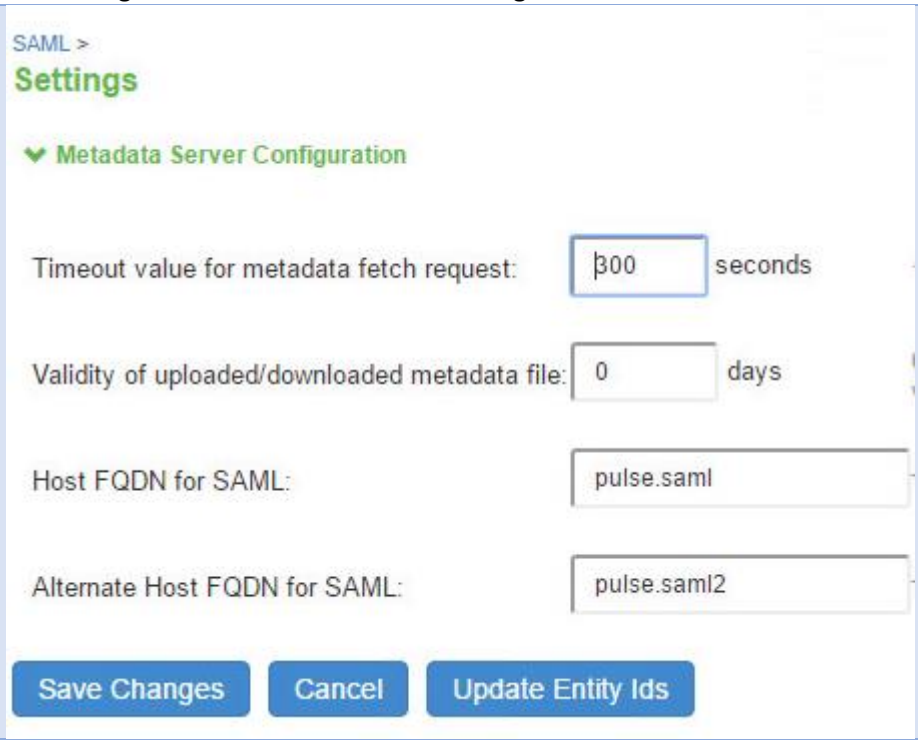


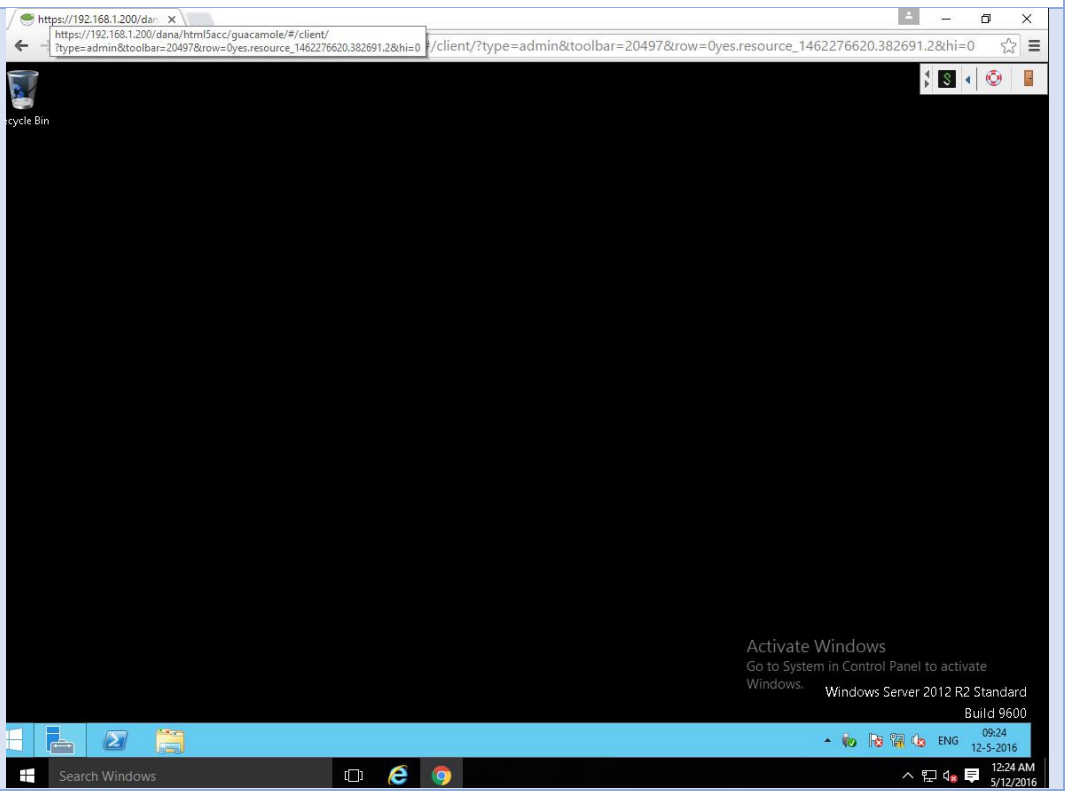
Lokale RDP sessie met extra optie.



ID	Test
G3	Is het mogelijk om een RDP sessie te starten vanaf de client?
Uitslag	Ja, dit kan op verschillende manieren geconfigureerd worden. Er kan een bookmark voor de user worden aangemaakt of de user wordt na het inloggen in de browser gelijk doorgezet naar de RDP sessie.
Bewijs	Eerst inloggen via de webbrowser. Vanuit de browser kiest de gebruiker om een Remote Desktop sessie te starten. Er worden credentials gevraagd.  Wanneer de gebruiker inlogt, wordt een sessie met de server opgezet. Hieronder is te zien dat user1 ingelogd is op de server met ip adres 192.168.1.1. 

ID	Test
G4	Is het eenvoudig om client software te installeren?
Uitslag	De Host Cecker software en Pulse Terminal Services Client worden automatisch geïnstalleerd. Hiervoor zijn geen administrator-rechten vereist.
Bewijs	 

ID	Test
G5	Is het mogelijk om gebruik te maken van SSO (Single Sign-On)?
Uitslag	Ja. SAML wordt gebruikt voor SSO en ACL (Access Control List). In onderstaande afbeelding is te zien dat SAML SSO te configureren is.
Bewijs	

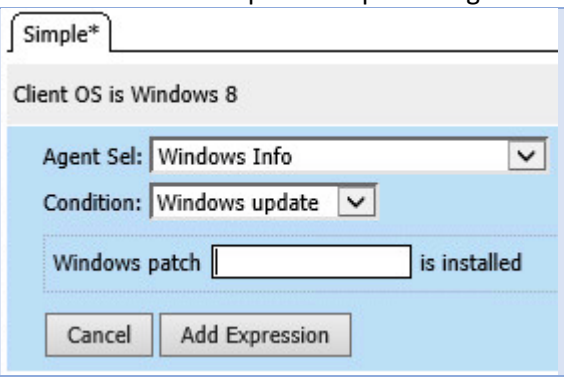
ID	Test
G6	Is het mogelijk om een RDP sessie binnen de browser te starten (HTML5)?
Uitslag	Ja, dit is eenvoudig te configureren. Hieronder ziet u dat Windows Server 2012 binnen de browser van een Windows 10 machine draait.
Bewijs	

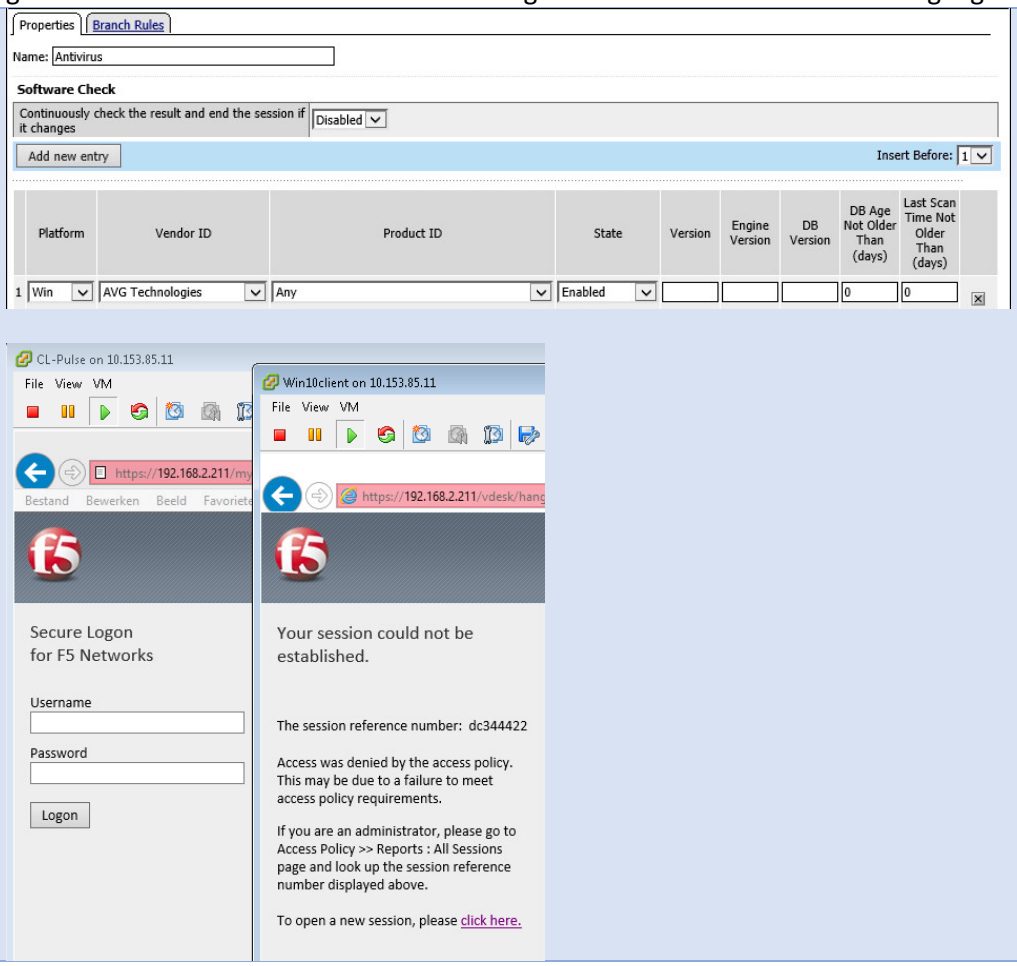
Score na test

Test	Score (0 t/m 10)	Weging (1 t/m 4)	Totaal
H1	6	3	18
H2	8	3	24
H3	10	3	30
H4	10	3	30
H5	10	3	30
H6	10	3	30
C1	10	4	40
C2	10	4	40
C3	10	4	40
C4	10	4	40
C5	8	4	32
T1	10	4	40
T2	10	4	40
T3	10	4	40
T4	10	4	40
G1	10	3	30
G2	0	4	0
G3	10	4	40
G4	10	4	40
G5	8	4	32
G6	10	4	40
Totaal	-	-	696

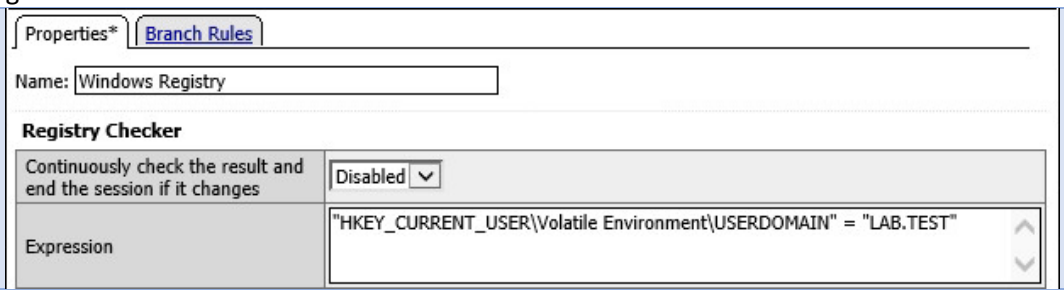
F5 Big-IP

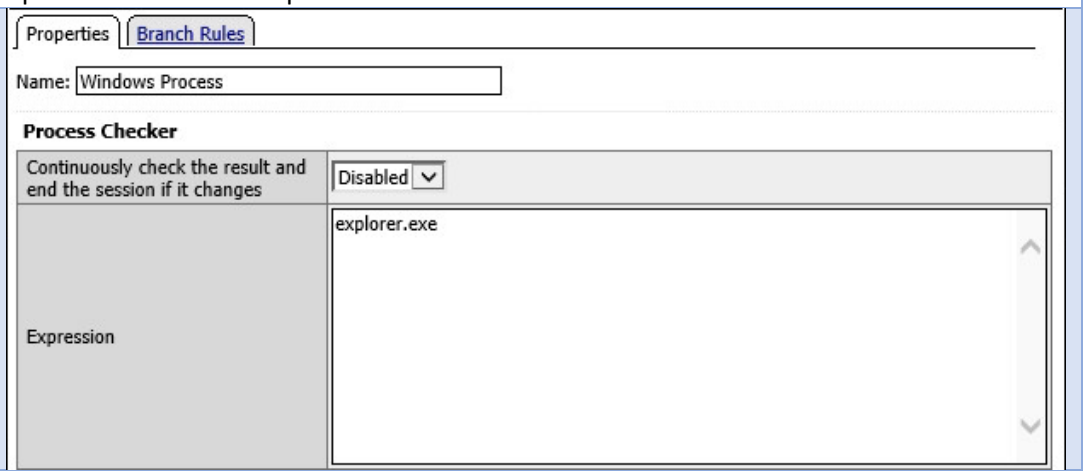
Hostcheck

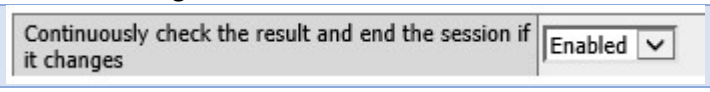
ID	Test
H1	Kan er gecontroleerd worden op Windows updates?
Uitslag	Ja, dit is eenvoudig te configureren via de APM. Er kan een rule per Windows versie worden gemaakt. Vervolgens kan er gekozen worden om Windows updates te controleren en een specifieke patch te geven.
Bewijs	

ID	Test
H2	Kan er gecontroleerd worden of er een antivirusprogramma aanwezig is?
Uitslag	Ja, zoals te zien is in de afbeelding hieronder kan er heel specifiek worden gecontroleerd op de antivirus. Zelf heb ik een rule gemaakt die controleert op Windows systemen of er een willekeurige versie van AVG Technologies aanwezig is. Op de Windows 10 client heb ik geen virusscanner geïnstalleerd. Op een andere Windows 8 client heb ik AVG Free geïnstalleerd. U ziet in de tweede afbeelding dat de Windows 8 client wel toegang krijgt.
Bewijs	

ID	Test
H3	Kan er gecontroleerd worden wanneer een laatste virusscan is uitgevoerd?
Uitslag	Ja, dit is eenvoudig aan te geven binnen APM.
Bewijs	

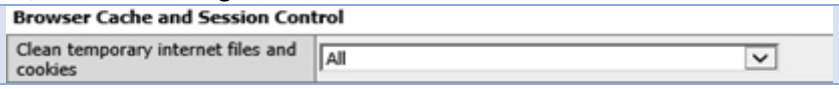
ID	Test
H4	Kan er gecontroleerd worden of de client lid is van het domein?
Uitslag	Ja, er kan een rule worden opgegeven waarbij een waarde binnen het register wordt gecontroleerd.
Bewijs	

ID	Test
H5	Kan er gecontroleerd worden welke processen er draaien?
Uitslag	Ja, er kan worden gecontroleerd op processen. We kunnen clients toestaan of afwijzen op basis van draaiende processen.
Bewijs	

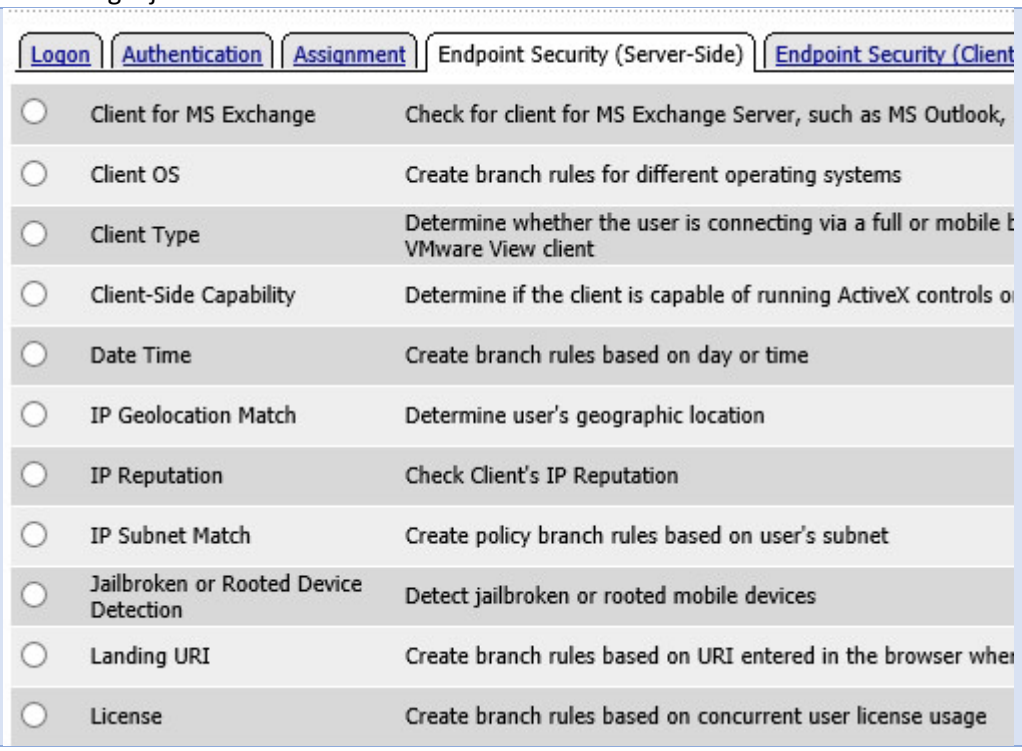
ID	Test
H6	Kan de hostcheck elke half uur worden uitgevoerd?
Uitslag	Nee. Wel kan er continu gecheckt worden. Wanneer een waarde veranderd, wordt de sessie beëindigd.
Bewijs	

Cache cleaning

ID	Test
C1	Kan de cache op de client worden verwijderd na een sessie?
Uitslag	Ja, Windows Cache kan eenvoudig worden verwijderd op de client. Hiervoor zijn vele opties binnen de APM.
Bewijs	

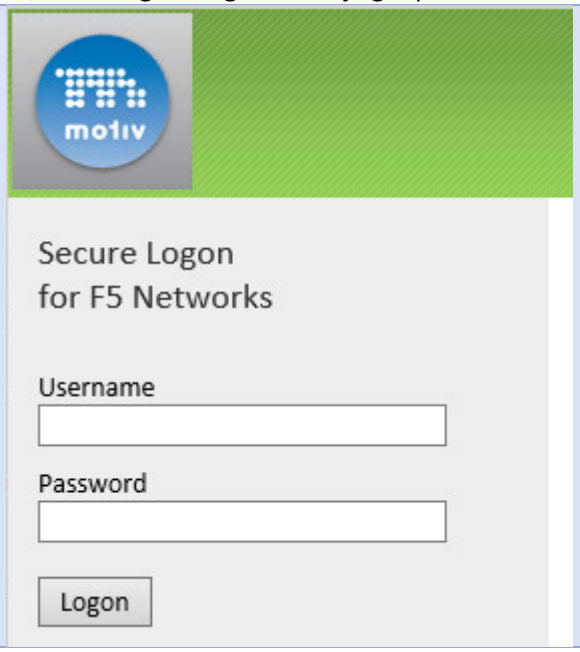
ID	Test
C2	Kunnen cookies automatisch na een sessie worden verwijderd op de client?
Uitslag	Ja, dit is eenvoudig in te stellen.
Bewijs	

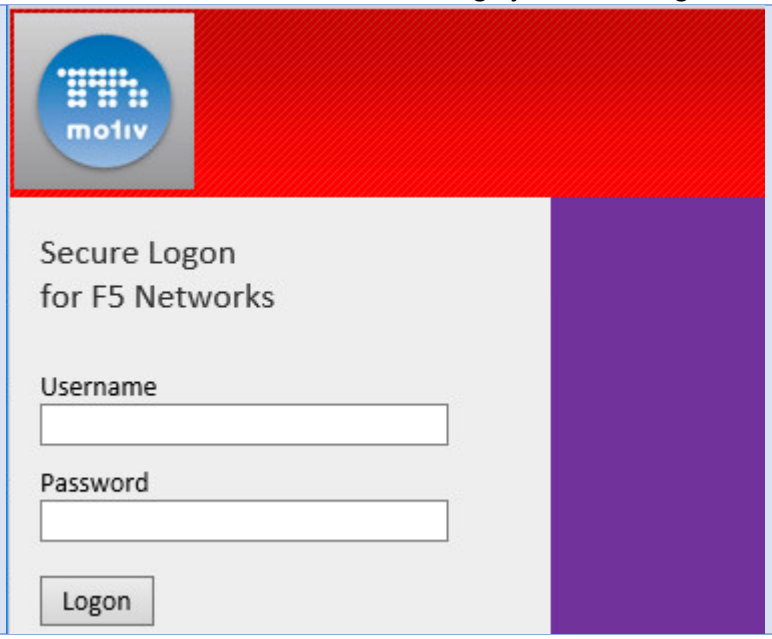
ID	Test
C3	Kunnen opgeslagen wachtwoorden automatisch na een sessie worden verwijderd op de client?
Uitslag	Ja, dit is wederom eenvoudig in te stellen onder Windows Cache and Session Control.
Bewijs	

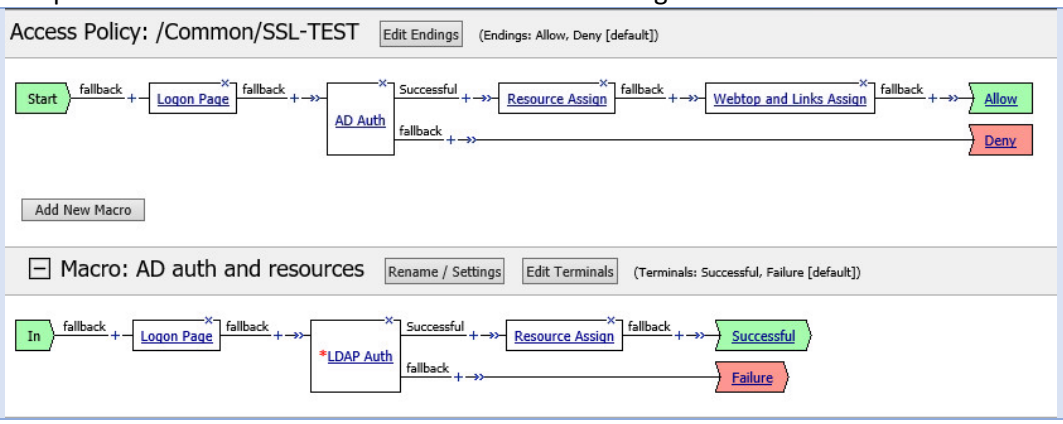
ID	Test
C4	Kan cache automatisch na een sessie worden verwijderd op de server?
Uitslag	Deze mogelijkheid is niet te vinden in de APM.
Bewijs	

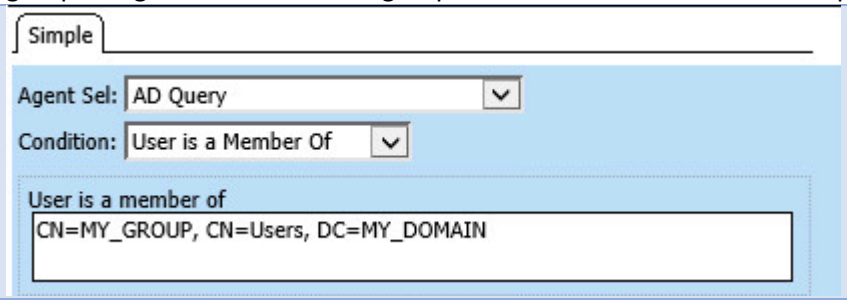
ID	Test
C5	Kunnen cookies automatisch na een sessie worden verwijderd op de server?
Uitslag	Deze mogelijkheid is niet te vinden in de APM. Zie bewijs C4.
Bewijs	N.v.t.

Technische functionaliteiten

ID	Test
T1	Kan er een logo worden weergegeven op de portal?
Uitslag	Ja, een image kan gemakkelijk geüpload worden via de webbrowser.
Bewijs	

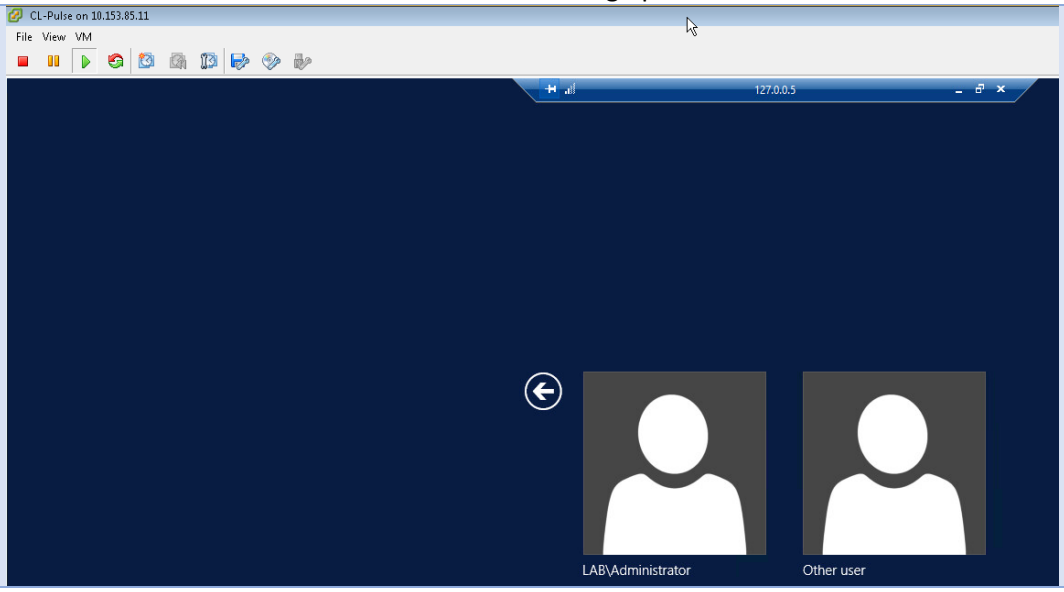
ID	Test
T2	Kan de achtergrond kleur worden aangepast van de portal?
Uitslag	Zoals te zien in onderstaande afbeelding zijn de kleuren gemakkelijk aan te passen.
Bewijs	

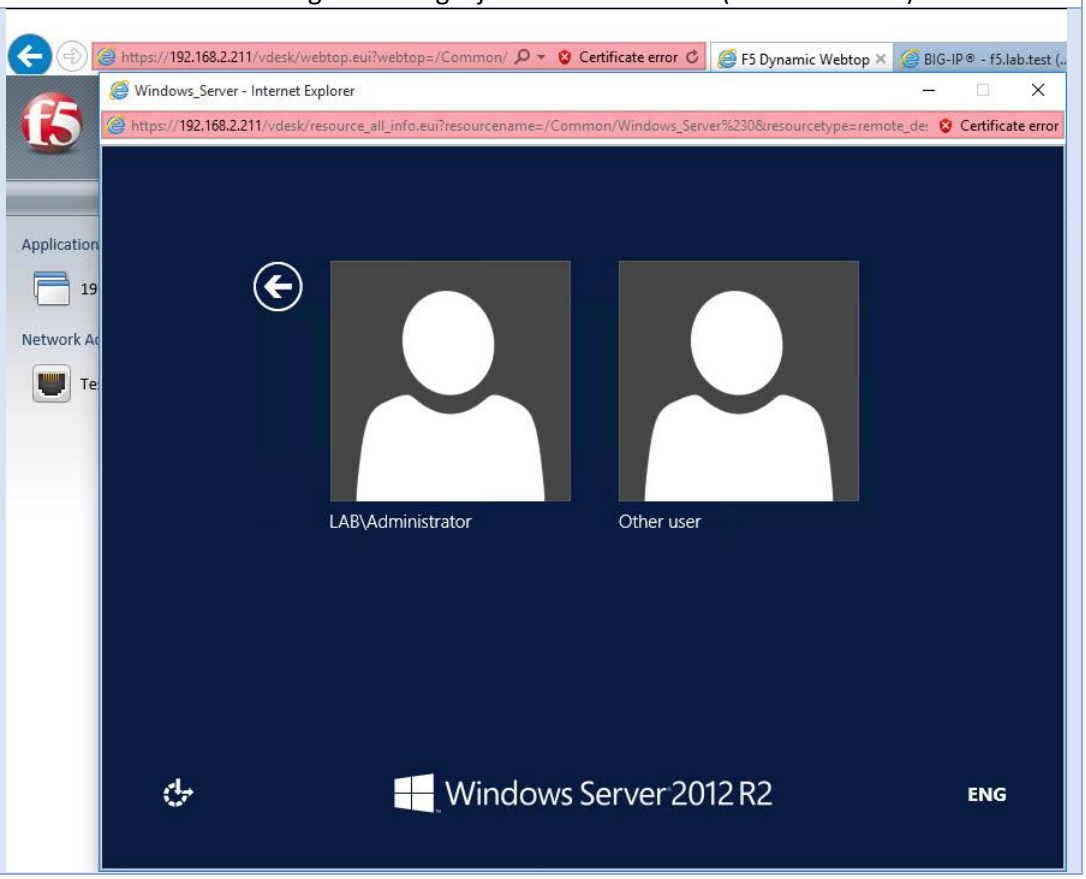
ID	Test
T3	Kunnen er verschillende rollen per authenticatiemethode worden toegepast?
Uitslag	Ja, er kunnen meerdere policies worden aangemaakt. Zo kan er gekozen worden voor meerdere portals of andere authenticatiemethoden. Per authenticatiemethode kunnen er op deze manier verschillende resources worden toegekend.
Bewijs	

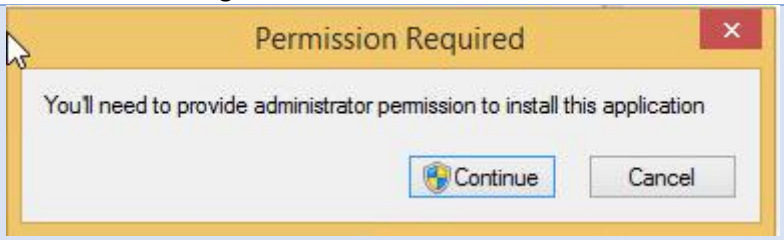
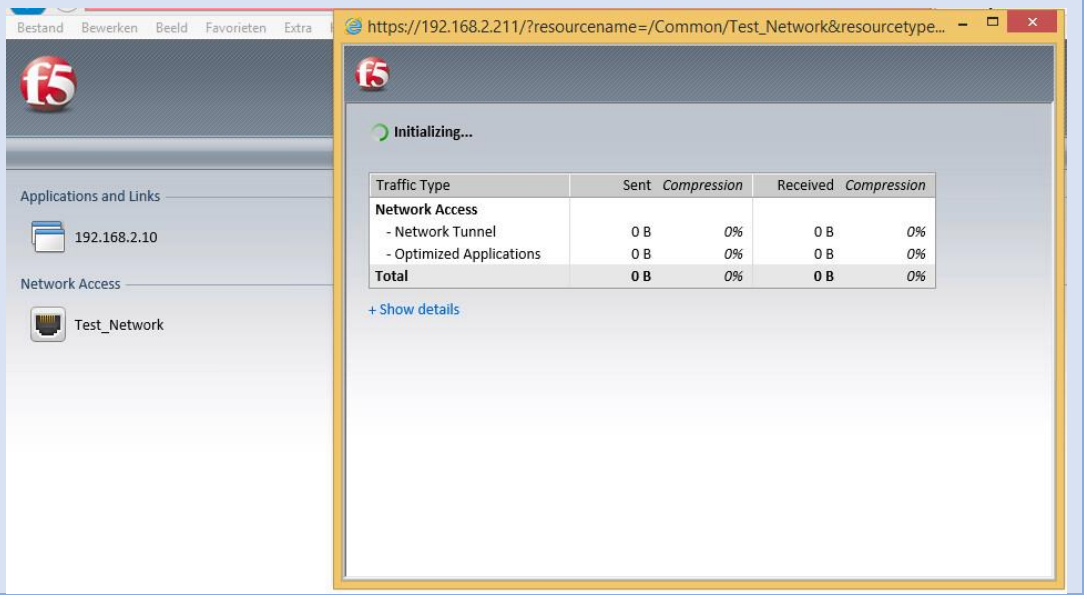
ID	Test
T4	Kunnen er verschillende rollen per gebruiker en per groep worden toegepast?
Uitslag	Ja, er kan een simpele regel worden aangemaakt waar wordt gecontroleerd bij welke groep een gebruiker hoort. Per groep kunnen er resources worden bepaald.
Bewijs	

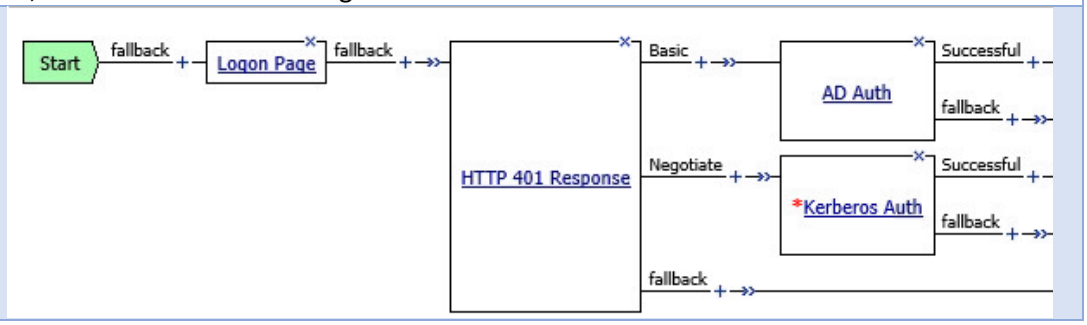
Gebruikerstest

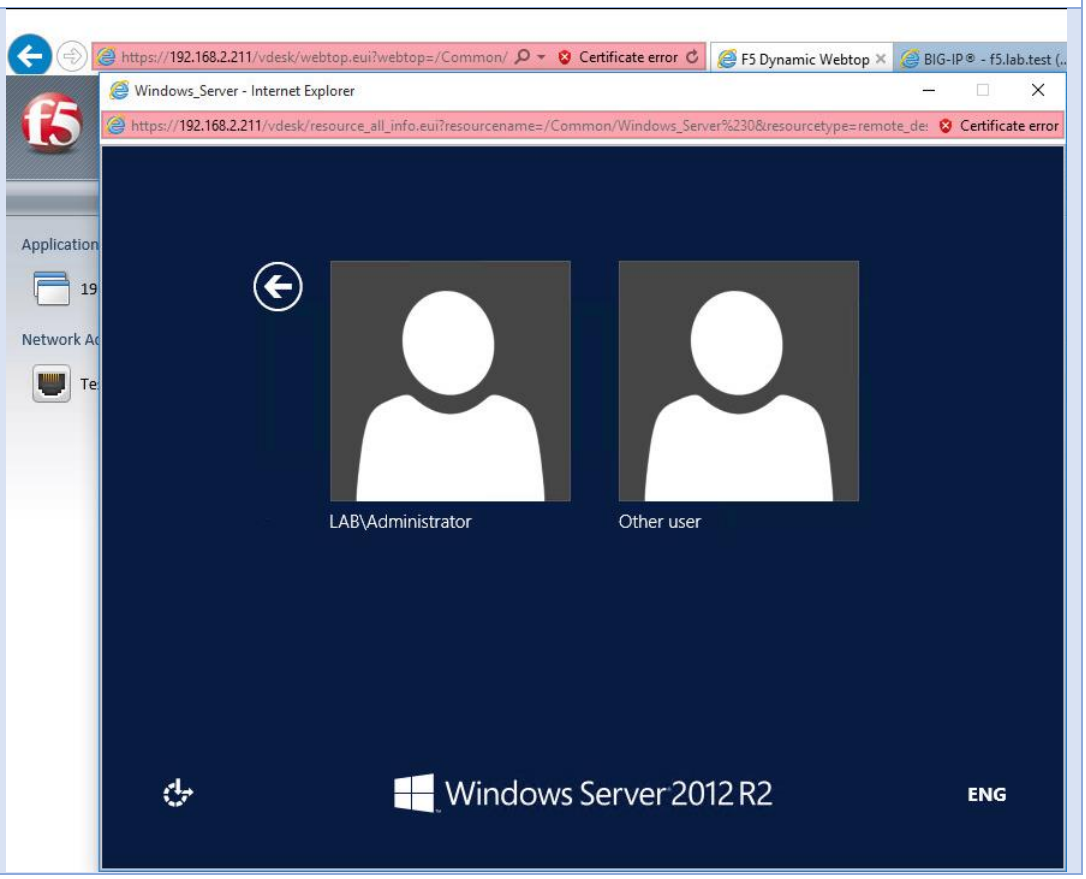
ID	Test
G1	Is er een mobiele pagina voor gebruikers met een smartphone of tablet?
Uitslag	Met de iPhone 6, iPad en Android krijgen we onderstaande mobiele pagina te zien.
Bewijs	

ID	Test
G2	Kan er gewerkt worden met meerdere monitoren?
Uitslag	Dit heb ik niet goed kunnen testen, aangezien de clients allemaal één monitor bevatten. Wel kan er met de F5 worden ingesteld dat RDP in full-screen mode kan worden gestart. Dit levert het resultaat uit onderstaande afbeelding op.
Bewijs	

ID	Test
G3	Is het mogelijk om een RDP sessie te starten vanaf de client?
Uitslag	Ja. Echter is het alleen nog maar mogelijk om dit via HTML5 (dus in browser) te doen.
Bewijs	

ID	Test
G4	Is het eenvoudig om client software te installeren?
Uitslag	De client software dient eenmaal geïnstalleerd te worden door de administrator. Vervolgens kan de plug-in gebruikt worden in de browser. Het maken van een netwerkverbinding vereist deze installatie.
Bewijs	 

ID	Test
G5	Is het mogelijk om gebruik te maken van SSO (Single Sign-On)?
Uitslag	Ja, via de APM is dit te configureren.
Bewijs	

ID	Test
G6	Is het mogelijk om een RDP sessie binnen de browser te starten (HTML5)?
Uitslag	Ja, zie onderstaande afbeelding. Hier wordt een sessie gestart naar de Windows Server vanaf de Windows 10 client.
Bewijs	

Score na test

Test	Score (0 t/m 10)	Weging (1 t/m 4)	Totaal
H1	10	3	30
H2	10	3	30
H3	10	3	30
H4	10	3	30
H5	10	3	30
H6	5	3	15
C1	10	4	40
C2	10	4	40
C3	10	4	40
C4	0	4	0
C5	0	4	0
T1	10	4	40
T2	10	4	40
T3	7	4	28
T4	7	4	28
G1	10	3	30
G2	0	4	0
G3	6	4	24
G4	5	4	20
G5	8	4	32
G6	10	4	40
Totaal	-	-	587