Take time to think
It is the source of all power
Take time to read
It is the fountain of wisdom

- Ecclesiates 3:1-8, author unknown[1]

TITELBLAD

Gegevens afstudeerder:	
Naam + voorletters:	Damen, S. (Stan)
Studentnummer:	2098311
Opleiding:	ICT: Management & Security, voltijd
Afstudeerperiode:	1 feb. 2010 t/m 8 jul. 2010 (100 werkdagen)

Gegevens bedrijf:	
Naam:	Vanderlande Industries B.V.
Afdeling:	IT Infra./Projects
Plaats:	Veghel, Nederland
Naam + voorletters bedrijfsbegeleider:	Jansen, M. (Maurice)
Functie:	Groupleader IT Infra./Projects
Naam + voorletters technisch begeleider:	Verbruggen, M. (Marcel)
Functie:	IT Project Engineer

Gegevens docentbegeleider:	
Naam + voorletters:	Wijnja, T. (Tiemen)
Instelling:	Fontys Hogeschool ICT
Plaats:	Eindhoven, Nederland

Gegevens afstudeerscriptie:	
Titel:	"The support link between Supplier and Customer" Onderzoek en ontwerp van een nieuwe remote support oplossing via VPN
Versie:	Final
Datum uitgifte:	9 jun. 2010 *Niet vertrouwelijk*

Fontys Hogeschool Informatica

VANDERLANDE® INDUSTRIES

Getekend voor gezien door:

Datum:

De bedrijfsbegeleider,

Datum:

De technisch begeleider,

VOORWOORD

Voor u ligt het resultaat van een interessante en leerzame periode: mijn afstuderen bij Vanderlande Industries in Veghel. Deze scriptie is geschreven als verantwoording van mijn werkzaamheden tijdens het afstuderen en om aan te tonen wat ik heb geleerd en hoe ik mij tijdens deze periode heb ontwikkeld.

Tijdens mijn afstudeerperiode heb ik een onderzoek uitgevoerd naar nieuwe mogelijkheden voor remote support via een “virtual private network”. Het onderzoek is uitgevoerd in de periode februari 2010 tot en met juni 2010 op de afdeling IT Infra./Projects van Vanderlande Industries.

Tijdens het zoeken naar een opdracht had ik mijzelf “verbreding van mijn kennis” als doel gesteld, naast de verdieping die tijdens een afstudeeronderzoek belangrijk is. Mijn focus kwam hiermee al snel op netwerken te liggen, een onderwerp dat tijdens mijn studie maar beperkt is behandeld. Ik wilde hier graag meer ervaring in op doen.

Tijdens het lezen van deze scriptie zult u hier en daar citaten en gezegdes tegenkomen van bekende en minder bekende personen, die mij hebben geïnspireerd tijdens het uitvoeren van mijn onderzoek en het schrijven van mijn scriptie. Een beknopte achtergrond van de personen achter de citaten is opgenomen als onderdeel van de literatuurlijst.

Ik hoop dat deze scriptie u een boeiende leeservaring kan bieden en hij daarnaast leerzaam is, zoals ik ook mijn afstudeerstage heb beleefd.

Veghel, juni 2010

Stan Damen

Index

Samenvatting

Deze scriptie is geschreven voor Vanderlande Industries (VI), als onderdeel van de studie IT: Management & Security.
VI is een bedrijf dat gespecialiseerd is in automatische systemen; zoals bagagesystemen op vliegvelden, sorteersystemen voor postbedrijven en distributiesystemen voor magazijnen en distributiecentra. VI heeft op deze markten een sterke positie opgebouwd en opereert verspreid over de hele wereld.

Het afstudeerproject is uitgevoerd in opdracht van de afdeling IT Infra./Projects. Deze afdeling valt onder de overkoepelende IT afdeling en is één van de vijf subafdelingen. IT Infra./Projects houdt zich bezig met projecten die gericht zijn op grootschalige wijzigingen aan de infrastructuur. De overige vier subafdelingen houden zich bezig met dagelijks beheer van de infrastructuur en interne software.

Om service en support te leveren op automatische systemen bij de klant, wordt gebruik gemaakt van remote support via een Virtual Private Network (VPN). Voor VPN worden veel verschillende oplossingen, methodes en softwarevarianten gebruikt, wat ervoor heeft gezorgd dat het VPN landschap erg divers is. Om te zorgen voor standaardisatie, een vereenvoudiging van beheerstaken en een hogere kwaliteit van service, is een nieuwe of verbeterde oplossing noodzakelijk voor VI.

De afstudeeropdracht bestaat uit het vinden en onderzoeken van deze nieuwe VPN oplossing(en) en het testen van de gevonden opties in de vorm van een Proof of Concept (PoC). Aan de hand van de resultaten van het onderzoek en de tests kunnen verdere stappen worden bepaald.

Om het afstudeerproject tot een goed einde te brengen is gekozen voor een indeling in fases, waarbij twee hoofdfases het grootste gedeelte van het project beslaan; de onderzoeksfase en de testfase.
In de onderzoeksfase is, door middel van een literatuurstudie, gekeken naar VPN technieken en methodes die in de situatie van VI bruikbaar konden zijn. Daarnaast is een lijst van eisen en wensen opgesteld, waaraan de nieuwe oplossing moest voldoen. Tijdens het onderzoek kwamen veel verschillende oplossingen aan bod, maar bleken de strenge eisen ervoor te zorgen dat weinig technieken voldeden. Uiteindelijk is er een selectie gemaakt van drie oplossingen; Cisco EasyVPN, Cisco AnyConnect en DMVPN. Cisco EasyVPN werd hierbij beschouwd als de meest geschikte kandidaat en geselecteerd voor de eerste PoC. De slagingskans van de Cisco EasyVPN oplossing werd het hoogste ingeschat en ook de benodigde apparatuur was beschikbaar. Op basis van de verwachte configuratie, verwachte slagingskans en het gebruik van SSL VPN tegenover IPSec VPN, is besloten om Cisco AnyConnect te testen in een tweede PoC. De DMVPN oplossing werd achter de hand gehouden, mochten beide andere oplossingen niet tot een positief resultaat leiden.

Tijdens de testfase zijn de twee PoC's uitgevoerd; de eerste met betrekking tot Cisco EasyVPN. Beide technieken zijn getest in twee globale stappen; de eerste stap was het testen van de benodigde basis connectiviteit om remote support te kunnen leveren. Als tweede stap is gekeken naar de overige eisen en wensen, zoals gedefinieerd in de lijst uit de onderzoeksfase. Cisco EasyVPN bleek alle benodigde functionaliteiten te bezitten en een oplossing te bieden voor VI. Als tweede PoC is Cisco AnyConnect getest, in combinatie met Policy Based Routing (PBR). In theorie konden deze twee technieken samen werken als VPN oplossing. Het bleek echter niet mogelijk PBR op de benodigde manier toe te passen, vanwege het gebruik van VPN en versleuteld dataverkeer. Hierdoor kon niet aan de eisen met betrekking tot de verbinding worden voldaan en dit heeft ertoe geleidt dat de Cisco AnyConnect oplossing afgewezen werd als mogelijkheid.
Vanwege een gebrek aan tijd, apparatuur en de lage slagingskans, is besloten om DMVPN niet meer in een PoC te testen.

De uiteindelijke conclusie van het afstudeerproject is tweeledig; Cisco EasyVPN biedt een goede oplossing voor de VPN problematiek bij VI. Het biedt veel kansen om te standaardiseren en vereenvoudigen. De tweede conclusie is dat het momenteel nog niet mogelijk is een SSL VPN oplossing te gebruiken die aan de eisen van VI voldoet. Cisco AnyConnect gecombineerd met PBR levert geen werkende situatie op. Wel heeft de tweede PoC kennis en inzicht opgeleverd die in een later stadium gebruikt kan worden.

Summary

This thesis is the result of my graduation internship performed at Vanderlande Industries, as part of my Bachelor of IT degree in IT: Management & Security.
VI is a global enterprise that specializes in automated systems in the markets of distribution, parcel & postal and baggage handling. In these fields, VI holds a leading position and has established a strong reputation.

The graduation project was performed at the IT Infra./Projects sub department, that is part of the IT department of VI. The IT Infra./Projects sub department focuses on changes to the infrastructure, that justify a project due to time and size requirements. Besides IT Infra./Projects there are four other sub departments, which focus on daily and software management.

To provide service and support on automated systems at various customer sites, VI uses remote support across Virtual Private Networks (VPN). Every customer has its own VPN connection. The amount of different VPN solutions used, leads to a diverse and difficult to manage environment. In order to attain a higher level of quality in providing service and to achieve standardization within VI, a new or improved solution is required.

The research conducted for this project was focused on finding and testing one or more new VPN solutions and provides a baseline for future steps, like implementation. The researched solutions were tested using a method called Proof of Concept (PoC) testing. After testing has been completed, further steps can be specified.

The graduation project was divided into two main phases; the research phase and the test phase.
In the research phase, a study was performed into current VPN techniques and possibilities. The second part of the phase focused on creating a list of demands/wishes, that the new solution must/should meet. This list was composed with the input of all parties involved, including service and support departments. Many of the solutions found during the research phase did not meet the basic demands of VI and were quickly discarded. At the end of the research phase, three solutions remained; Cisco EasyVPN, Cisco AnyConnect and DMVPN. Only the first two solutions were tested in a PoC, due to the estimated chance of success and complexity. Cisco EasyVPN had the highest estimated chance of success, which is the main reason it was tested first. All necessary equipment was also available. Cisco AnyConnect is the only solution that uses SSL VPN, as opposed to IPSec VPN, which could be a strong advantage. For this reason it was tested in the second PoC. DMVPN was kept as a back-up solution in case the two aforementioned solutions proved unfeasible.

In the test phase two PoCs were performed, the first one concerning Cisco EasyVPN and the second utilizing Cisco AnyConnect. Both techniques were tested in two steps; the first step concentrated on the basic connectivity required to use the solution for remote support, the second step focused on determining if the solutions were capable of meeting the demands and wishes, specified in the research phase.

The Cisco EasyVPN solution proved to meet all items on the list and could provide a good solution for VI.
The Cisco AnyConnect solution was combined with Policy Based Routing (PBR), as a result of the findings from the first PoC. PBR was intended to provide a way back for VPN traffic, which turned out to be difficult with the Cisco EasyVPN solution. However, PBR proved not to work with VPN tunnels, because of the encrypted traffic involved, and therefore the Cisco AnyConnect solution did not meet the basic connectivity demands.
The DMVPN solution was not tested due to a lack of time, equipment and a low estimated chance of success.

Two conclusions can be drawn from the research and test results;
Cisco EasyVPN provides a good solution that meets the VI demands and has several benefits as opposed to the current solutions. By properly implementing the solution, it should be possible to achieve better quality of service and a higher level of standardization.
The second conclusion is that Cisco AnyConnect cannot be used as a solution for VI and that it is not possible to use SSL VPN for VI, with the current techniques available. Testing with Cisco AnyConnect and PBR did provide insight in PBR capabilities, which could possibly be used in the future.

Verklarende woordenlijst

Begrip	Betekenis
Access Control List (ACL)	Een ACL is een lijst met permissies en/of restricties met betrekking tot bijvoorbeeld netwerk- of bestandstoegang.
Customer controlled client-server (CCCS)	Een VPN oplossing waarbij gebruik gemaakt wordt van de bestaande client-server VPN oplossing van een klant.
Customer controlled site-to-site (CCSS)	Een VPN oplossing waarbij gebruik wordt gemaakt van de site-to-site VPN oplossing van een klant.
Direct Modem (DM)	Een (legacy) remote access oplossing die gebruik maakt van modems en telefoonlijnen.
Dynamic Multipoint VPN (DMVPN)	Een Cisco VPN techniek die gebruik maakt van een "hub-spoke" opstelling.
EasyVPN	Een Cisco VPN techniek die gebruik maakt van de client-server architectuur, maar de eigenschappen van een site-to-site VPN nabootst.
Information Technology (IT)	Het vakgebied dat zich bezighoudt met Informatie, Communicatie en Technologie, gelijk aan ICT.
Internet Protocol (IP)	Een belangrijk onderdeel van het systeem dat computernetwerken gebruiken om met elkaar te communiceren.
Network Address Translation (NAT)	Een techniek die bedoeld is om een IP adres te vertalen naar een ander (publiek) IP adres.
Network Extension Mode (NEM)	Een functionaliteit van EasyVPN die gebruikt wordt om een site-to-site VPN na te bootsen.
Policy (groeps-)	Een set van regels of instellingen die bepalen hoe de configuratie van bijvoorbeeld een VPN-client er uit gaat zien.
Programmable Logic Controller (PLC)	Een elektronisch apparaat met een microprocessor, die gebruikt wordt in de aansturing van automatische systemen.
Proof of Concept (PoC)	Een test om te bepalen of een concept in de praktijk kan werken. Deze tests worden, over het algemeen, uitgevoerd in een testomgeving.
Register	Het Windows register is een database met instellingen van het besturingssysteem, applicaties, gebruikers en apparaten.
Remote Access Program for Interactive Diagnostics (RAPID)	Een door FEI ontwikkelde applicatie die gebruikt wordt om op afstand elektronische microscopen te beheren.
Remote Desktop Protocol (RDP)	Een netwerkprotocol dat gebruikt wordt om van afstand verbinding te maken met een computer.
Router	Een apparaat dat gebruikt wordt om data over een netwerk naar de juiste locatie te sturen.
Secure Socket Layer VPN (SSL VPN)	Een VPN oplossing die gebruik maakt van het standaard SSL netwerk protocol om een verbinding op te zetten, bijvoorbeeld via een web browser.
Service Distribution, Parcel & Postal (DPP)	Een afdeling binnen Vanderlande Industries die zich bezighoudt met service en reserveonderdelen voor systemen bij klanten.
Smart card/Token	Een geavanceerde vorm van authenticatie, waarbij een object gebruikt wordt dat in het bezit is van de gemachtigde persoon. Bijvoorbeeld een smart card die in de kaartlezer van de computer gestoken moet worden of een token dat een cijfercode genereert (e.g. Rabobank random reader).
Vanderlande controlled client-server (VCCS)	Een VPN oplossing waarbij gebruik gemaakt wordt van een client-server VPN oplossing beheerd door Vanderlande Industries.
Vanderlande controlled site-to-site (VCSS)	Een VPN oplossing waarbij gebruik wordt gemaakt een site-to-site oplossing, opgezet en beheerd door Vanderlande Industries.
Virtual Private Network (VPN)	Een privé netwerk met een verbinding naar een secundair(e) netwerk/gebruiker, waarbij een veilige en vertrouwde connectie wordt opgezet tussen deze twee.

1. Inleiding

Een Virtual Private Network (VPN)* is een techniek om een gebruiker of netwerk, op afstand te verbinden met een (ander) netwerk. Doorgaans gebeurt dit over een publiek netwerk, zoals het Internet, maar met behoudt van *veiligheid* en *vertrouwelijkheid*. En die twee begrippen zijn de kern van VPN: door gebruik te maken van een veilige verbinding met een netwerk, wordt gezorgd voor vertrouwde toegang tot de componenten in dat netwerk. VPN bestaat sinds de jaren '90 en heeft een grote invloed uitgeoefend op de ontwikkeling van netwerken binnen bedrijven, de overheid, instellingen en in sommige gevallen ook thuisgebruikers. Met VPN werden mogelijkheden gecreëerd die voorheen niet bestonden.

Vanderlande Industries (VI) is een bedrijf dat automatische systemen, zoals bagagesystemen, ontwikkelt en plaatst bij klanten over de hele wereld. VI maakt gebruik van VPN voor het leveren van ondersteuning op afstand, het zogenaamde remote support. Vanuit de vestigingen van VI worden de systemen bij klanten, indien mogelijk, gerepareerd en onderhouden. De verbinding die gebruikt wordt om bij deze systemen te komen moet veilig zijn; de vertrouwelijkheid van data die over de verbinding wordt verstuurd mag niet in gevaar komen. Om dit te waarborgen was het voor VI een logische stap om VPN's te gebruiken voor deze verbindingen.

Er zijn meerdere types VPN die allemaal verschillende voor- en nadelen hebben. Binnen VI wordt er gebruik gemaakt van verschillende oplossingen voor VPN, maar geen is ideaal. Dit komt voornamelijk door de wensen en eisen van de klant, of door de technische mogelijkheden die voor een specifieke klant gelden. Het resultaat is een grote verzameling verschillende VPN verbindingen, die allemaal net anders werken, en een grote collectie bijbehorende handleidingen. Het gevolg is een onoverzichtelijk geheel van technieken, merken en oplossingen.

Deze grote verscheidenheid is de oorzaak van een aantal problemen; het ontbreken van een standaard oplossing en het grote aantal handleidingen bemoeilijkt het werk van engineers die ondersteuning leveren aan klanten (support engineers) en beheerders. Ook wordt er in veel gevallen gebruik gemaakt van de bestaande VPN oplossing bij de klant. Dit vergroot de klantafhankelijkheid van VI en kan het leveren van remote support belemmeren. Uiteindelijk zorgt dit ook voor een afname in de kwaliteit en efficiëntie van de service.

Om dit probleem aan te pakken moesten er meerdere fases doorlopen worden. Er moest een (literatuur)onderzoek worden gedaan naar mogelijke oplossingen. Deze werden daarna beoordeeld aan de hand van een lijst van eisen en wensen. Als laatste moest(en) de gekozen oplossing(en) worden getest in een Proof of Concept (PoC)* en werd over het totaal een advies gegeven. Deze verschillende fases zijn terug te vinden in deze afstudeerscriptie.

De opbouw van deze afstudeerscriptie is als volgt: in hoofdstuk 2 volgt een beknopte achtergrond over het bedrijf. Hoofdstuk 3 gaat uitgebreider in op de opdracht en de achtergrond van de opdracht. In de hoofdstukken daarna worden de verschillende fases van het afstudeerproject behandeld, beginnende in hoofdstuk 4 met het onderzoek. In hoofdstuk 5 worden de uitgevoerde PoC's behandeld, waarna in hoofdstuk 6 een conclusie wordt getrokken. Uiteindelijk wordt in hoofdstuk 7 een advies gegeven over eventuele vervolgstappen.

Een laatste opmerking: de aanduiding "[1]" duidt op een gebruikte bron, te vinden in de literatuurlijst. Het referentieteken "*" wordt gebruikt om aan te geven dat een term is opgenomen in de verklarende woordenlijst.

2. Bedrijfsbeschrijving

"In a World of Technology, a belief in People"

- Vanderlande Industries

2.1. Inleiding

Bovenstaande slogan geeft goed weer wat de kernwaarden zijn van VI, waar zij in geloven en waar zij voor staan. Vertaald staat er: "Vertrouwen in mensen, in een technologische wereld".

VI is een bedrijf dat zich richt op automatische systemen, maar wil daarbij de mensen achter deze systemen niet vergeten. VI heeft verschillende kernwaarden en uitgangspunten waarbinnen zij opereren. Deze kernwaarden zijn: Integriteit, Teamwork, Professionaliteit, Innovatie, Respect voor mensen, Respect van privacy en Zorg dragen voor goede arbeidsomstandigheden. Deze visie heeft een groot aandeel in de reputatie die VI heeft opgebouwd bij klanten en partners en is medeverantwoordelijk voor de groei in de wereldmarkt. In dit hoofdstuk worden kort het ontstaan van VI, de verschillende markten waarbinnen zij opereert en de afdeling waarbinnen dit afstudeerproject is uitgevoerd behandeld.

2.2. Ontstaan en groei van Vanderlande Industries

VI is begonnen opgericht in 1949 door de familie Van der Lande als een klein familiebedrijf. Het bedrijf is begonnen als een machinefabriek met als standplaats Veghel. Langzaam maar zeker is VI uitgegroeid tot één van de grotere bedrijven in de markt. Vooral in de eerste jaren van de 21e eeuw was er sprake van een groeispurt. Tegenwoordig, in 2010, heeft VI meer dan 2000 werknemers en vestigingen in alle belangrijke regio's van de wereld. Buiten de hoofdvestiging in Veghel, heeft VI vestigingen in België, Duitsland, Frankrijk, Italië, Groot-Brittannië, Spanje, Canada, De Volksrepubliek China, India, Zuid-Afrika en de Verenigde Staten[1]. Alle vestigingen, met uitzondering van de hoofdvestiging in Veghel, worden "Customer Centres" genoemd. Deze Customer Centres zijn een goed voorbeeld van de groei die het bedrijf heeft gemaakt over de afgelopen jaren. De verwachting is dat VI deze groei kan doorzetten en zich ook op andere plaatsen gaat vestigen, bijvoorbeeld in het werelddeel Zuid-Amerika.

2.3. Markten

Tegenwoordig is VI actief op drie verschillende markten: **Bagageafhandeling**, **Distributiesystemen** en **Parcel & Postal**[2]. In deze markten heeft VI een goede positie, maar vooral in de bagageafhandeling is het aandeel van VI groot: 2e op de wereldranglijst.

Bagageafhandeling
Bagageafhandeling is de afgelopen jaren een steeds grotere markt geworden. Vliegvelden groeien gestaag en het aantal passagiers en stuks bagage stijgt mee. VI levert bagage-afhandelingssystemen voor luchthavens, van de allergrootste tot de allerkleinste. De systemen die gemaakt worden, zijn gericht op betrouwbaarheid en effectiviteit tegen lage kosten.

Distributiesystemen
In de markt van distributiecentra systemen levert VI zijn aandeel met een groot scala aan producten. Zo leveren zij opslagsystemen, sorteersystemen en transportsystemen, maar ook automatische magazijnen en ondersteunende diensten. Deze diensten zijn gericht op het creëren van een hogere productiviteit en vooral gebruiksgemak; hierdoor heeft een nieuwe medewerker een inwerktijd van ongeveer 15 minuten. In deze markt behoort VI tot de top 5 van Europa, met meer dan 1000 gerealiseerde projecten.



Parcel & Postal
De laatste markt waar VI actief in is, is Parcel & Postal. In deze markt richt VI zich op technologieën en systemen voor het verwerken en sorteren van pakketten, documenten en post. De systemen die hiervoor worden gebruikt variëren van het grootste sorteerpunt ter wereld (200.000 pakketten per uur), tot kleine lokale postcentra met 1000 of meer pakketten per dag.

Bij al deze systemen kan VI volledige operationele ondersteuning bieden. Deze service richt zich op onderhoud, trainingen en procesondersteuning. Service is dan ook één van de kernactiviteiten van het bedrijf.

2.4. Afdeling Information Technology (IT)*

De IT afdeling is de overkoepelende afdeling waarbinnen dit afstudeerproject wordt uitgevoerd. De afdeling IT bestaat uit ongeveer vijftig medewerkers. Binnen de afdeling IT bestaan verschillende subafdelingen: Business Information Systems (BIS), Technical Information Systems (TIS), Workflow Information Systems (WIS), IT Infra./Projects en IT Infrastructure. Dit afstudeerproject is uitgevoerd als onderdeel van de subafdeling IT Infra./Projects.

IT Infra./Projects is de subafdeling die zich bezig houdt met grootschalige wijzigingen aan de infrastructuur. Deze wijzigingen worden als project opgepakt vanwege de omvang en de daarvoor benodigde tijd. Een tweede onderwerp waar IT Infra./Projects zich mee bezig houdt zijn projecten gericht op het plaatsen van systemen bij nieuwe klanten.

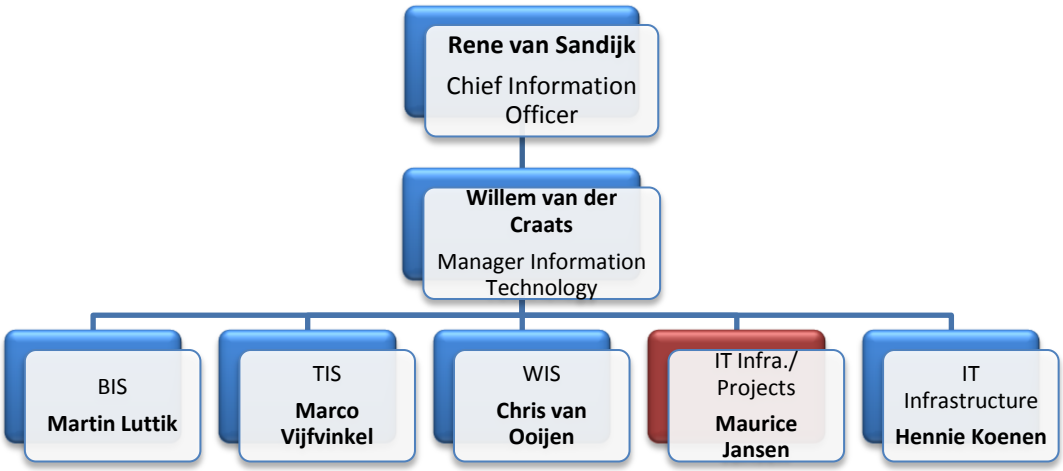
De andere subafdelingen binnen de afdeling IT houden zich bezig met het ICT beheer: WIS met de bedrijfsproces ondersteunende software, TIS ontwikkelt de specifieke technische software die gebruikt wordt bij het ontwerpen van VI systemen, BIS met de ERP-software en IT Infrastructure met het beheren van werkplekken, servers en overige software. Binnen de subafdeling IT Infrastructure valt ook de Service Desk. Hier worden interne incidenten, service requests, etc. ingediend en (indien mogelijk) afgehandeld.

2.5. Afdelingen Control Support en Service Distribution, Parcel & Postal (Service DPP)*

De afdelingen die niet direct binnen IT vallen, maar wel belangrijk waren voor dit afstudeerproject zijn Control Support en Service DPP. Deze afdelingen maken gebruik van de VPN oplossingen. Zij leveren de remote support aan klanten en handelen externe incidenten en service requests af.

2.6. Organigram afdeling Information Technology

Onderstaand een beknopt organigram van de afdeling IT. De subafdeling IT Infra./Projects is donker rood aangegeven.



Figuur 1: organigram IT afdeling

3. Projectbeschrijving

3.1. Inleiding

Wat is de huidige situatie? Hoe ziet het VPN landschap eruit? Wat voor problemen creëert dit en waarom? Welke partijen zijn betrokken bij het netwerk en VPN? Wat zijn de doelstellingen en de scope van het project?

Op bovenstaande vragen wordt in dit hoofdstuk een antwoord gegeven. Ook wordt de achtergrond van het project en de opdracht verduidelijkt om precies aan te geven met welke gedachtegang de opdracht is geformuleerd en waarom aan het project is begonnen. Om een goede analyse te geven van de huidige situatie en het probleem wordt er gebruik gemaakt van één van de basismethodes voor analyse; 5xW+H, misschien beter bekend als "Wie, Wat, Waar, Waarom, Wanneer en Hoe".

3.2. Wat is de beginsituatie?

In de huidige situatie beheert VI ongeveer 120 klanten via VPN. Hierbij wordt in twee derde van de gevallen gebruik gemaakt van de bestaande oplossing voor VPN die de klant heeft; veel klanten hebben hun eigen specifieke VPN oplossing. Omdat er veel verscheidenheid tussen de mogelijkheden is, ontstaat er een VPN landschap met veel diversiteit. Deze verschillen zorgen voor problemen bij het beheren van de verbindingen, maar ook bij het leveren van remote support.

Binnen VI worden momenteel vier verschillende manieren gebruikt om VPN connecties op te zetten naar de klant ten behoeve van remote support. Ook wordt er in een paar gevallen nog gebruik gemaakt van een modem oplossing voor remote access. Deze vijf oplossingen zijn: "Direct Modem (DM)*", "Customer controlled client-server (CCCS)*", "Vanderlande controlled client-server (VCCS)*", "Customer controlled site-to-site (CCSS)*" en "Vanderlande controlled site-to-site (VCSS)*". Deze vijf oplossingen hebben allemaal specifieke voor- en nadelen. Gelet op de huidige groei van het aantal klanten en daarmee het aantal benodigde connecties, is geen van de oplossingen ideaal.

Zoals eerder vermeld, wordt in de meeste gevallen (65%) gebruik gemaakt van de CCCS oplossing. Bij deze oplossing ligt het grootste probleem bij de diversiteit die wordt gecreëerd en bij de klantafhankelijkheid. De afhankelijkheid is bij deze oplossing groot, zoals te zien is in tabel 1 hieronder.

	Initiatie	Snelheid	Klantafhanke-lijkheid	Eisen aan de infrastructuur	Kosten	Complexiteit	Schaalbaarheid	Veiligheid
Direct Modem	+	-	++	+	++	++	--	--
Customer controlled client server	-	+	-	-	+	-/+	-/+	+
Vanderlande controlled client server	-	+	+	+	-/+	-/+	+	+
Customer controlled site-to-site	+	+	-	-	+	-	-/+	-
Vanderlande controlled site-to-site	+	+	+	+	-/+	-	-/+	-

Tabel 1: vergelijkingstabel huidige oplossingen[3]

De DM oplossing heeft als grootste nadelen de snelheid, schaalbaarheid en beveiliging. Dit komt voornamelijk door het gebruik van een modem, en dus van de telefoonlijn. Er worden binnen VI nog maar weinig DM oplossingen gebruikt; het huidige aantal ligt op 5 stuks. Het is de bedoeling dat deze, wanneer mogelijk, worden gemigreerd naar een nieuwe oplossing.

Beide site-to-site oplossingen kampen met hetzelfde probleem: schaalbaarheid. Het is belangrijk om bij een site-to-site oplossing te kijken naar heel VI. De problemen met deze oplossing ontstaan zodra de Internet Protocol (IP)* adresseringsschema's bij twee klanten overeen komen. Er ontstaat dan een conflict waarvoor bij de site-to-site techniek geen oplossing is. De VPN server kan niet bepalen naar welk klantnetwerk de data gestuurd moet worden. Omdat het aantal klanten blijft groeien, kunnen er problemen ontstaan met deze nieuwe klanten. Ook veiligheid is bij deze oplossing een probleem. Gebruikersauthenticatie kan wel worden toegepast op de VPN tunnel, maar in de praktijk is dit niet geïmplementeerd. Dit betekent dat beide netwerken volledig voor elkaar toegankelijk zijn, voor iedereen die zich in één van de twee netwerken bevindt.

Initiatie is een probleem dat geldt voor beide client-server oplossingen. Met initiatie wordt bedoeld dat de verbinding opgezet moet worden vanuit VI, richting de VPN server bij de klant. Hiervoor moeten inkomende verbindingen worden toegestaan door het netwerk van de klant. Site-to-site oplossingen hebben dit probleem niet, aangezien een site-to-site VPN tunnel van beide kanten kan worden gestart. Modem oplossingen maken gebruik van één modem aan elke zijde, wat ervoor zorgt dat de verbinding ook van beide kanten kan worden opgezet.

Op dit moment is de beste oplossing, gezien vanuit VI oogpunt, de VCCS oplossing. Hierbij komt er wel een client-server verbinding te staan, maar wordt deze beheerd en ingericht door VI. Dit zorgt voor een lage klantafhankelijkheid. Ook ontstaan er bij de client-server techniek geen problemen met schaalbaarheid, zoals bij site-to-site. Bij ongeveer 35 van de huidige klanten, wordt de VCCS oplossing gebruikt.

Een extra factor die bijdraagt aan de huidige problemen is het interne beleid. Momenteel wordt de IT-afdeling pas laat betrokken bij het proces van afspraken maken met een nieuwe klant. Dit betekent dat er vaak al afgesproken is welke VPN oplossing gebruikt gaat worden en hoe het IT gedeelte ingericht gaat worden, voordat de IT-afdeling hier een mening en advies over kan geven. Hierdoor is het moeilijk om klanten na de eerste onderhandelingen nog over te halen gebruik te maken van VCCS, als eerder voor een andere oplossing is gekozen.

3.3. Wie zijn de belanghebbenden?

Bij dit project is er sprake van verschillende belanghebbenden. Het gaat dan om de afdeling IT Infra./Projects en de afdelingen Control Support en Service DPP. Hierbij is een duidelijk onderscheid te maken; IT Infra./Projects regelt het opzetten en documenteren van nieuwe VPN verbindingen, alsmede het beheer van bestaande verbindingen. Control Support en Service DPP maken gebruik van de VPN verbindingen voor het leveren van support en service. Hierdoor is het meteen duidelijk dat beide groepen (beheerders en gebruikers) verschillende belangen hebben en dus andere aspecten belangrijk vinden; een belangrijk gegeven voor het opstellen van de lijst van eisen tijdens het onderzoek.

Uiteraard is de klant ook een belanghebbende; uiteindelijk moet de oplossing niet alleen voordeel opleveren voor VI, maar ook voor (nieuwe) klanten.

3.4. Waarom wordt het project uitgevoerd?

Om te bepalen wat de doelen zijn van dit afstudeerproject is het handig om te kijken naar de huidige problemen, en een oplossing voor die problemen mee te nemen als doel in het project.

Gekeken naar de eerder beschreven problemen, vertalen deze zich in de volgende doelen:

- Een betere schaalbaarheid om de verwachte groei van het aantal klanten aan te kunnen.
- Verbetering van de beheerbaarheid van de complete verzameling van VPN oplossingen door middel van een vergrote standaardisatie.
- Een verbetering van de service capaciteiten en kwaliteit, geleverd door de Control Support en Service DPP afdelingen aan de klant.
- Vergroting van het gebruiksgemak voor alle betrokkenen, zowel klanten als interne gebruikers, en hiermee bijdragen aan de kwaliteit van support en verbetering van de service.

3.5. Wat is de opdrachtdefinitie?

Om een inefficiënte en onwerkbare situatie te voorkomen is het noodzakelijk dat er een nieuwe oplossing wordt gevonden voor het leveren van remote support via VPN. Deze oplossing moet voldoen aan strikte eisen die in overleg met de betrokken partijen worden vastgelegd.

De opdracht voor dit afstudeerproject bestaat dus uit verschillende onderdelen:
Allereerst wordt er gezocht naar een oplossing die de huidige problemen zoveel mogelijk kan oplossen of beperken. Een oplossing die de positieve kanten van de huidige oplossingen heeft, maar geen van de negatieve kanten.
Ten tweede wordt gezocht naar een standaard, waarbij de technieken (en dus ook de handleidingen) gelijk zijn voor elke klant. Dit betekent dat de oplossing ook acceptabel moet zijn voor de klant.
Ten derde moet er gelet worden op de klantafhankelijkheid van VI; deze moet zoveel mogelijk worden beperkt.
Een oplossing die aan deze eisen voldoet, zorgt impliciet voor een toename in kwaliteit en efficiëntie van remote support.

3.6. Hoe wordt het project aangepakt?

Globaal bestaat het project uit drie delen: een onderzoek, een PoC en uiteindelijk een advies. De aanpak is onderverdeeld in twee fases: een onderzoeksfase en een testfase. De onderzoeksfase omvat het zoeken naar een oplossing en het opstellen van de lijst met eisen en wensen. De testfase omvat de PoC en het advies.

In totaal duurde de afstudeerperiode 20 weken. Voor de onderzoeksfase waren 6 weken uitgetrokken in de planning en voor de testfase 9 weken. De overige weken zijn gebruikt voor de opstart en afronding van het afstudeerproject. In de planning zijn ook de documenten opgenomen die zijn opgeleverd: het Project Initation Document (PID), het onderzoeksdocument, het testrapport en uiteindelijk deze afstudeerscriptie. De vooraf opgestelde planning is terug te vinden in het PID.

Uitgebreidere informatie over beide hoofdfases is te vinden in respectievelijk hoofdstuk 4 en 5. Het PID is toegevoegd als bijlage I.

3.7. Wat behoort tot de scope van het project?

Binnen het afstudeerproject vallen het onderzoek, de PoC en het geven van een conclusie/advies. Er wordt gekeken naar de functionaliteit van de oplossing en of deze voldoet aan de gestelde eisen.

Een belangrijk deel dat buiten de scope valt is het implementatieproces. Implementatie is een stap die na een besluit over het advies genomen kan worden. Ook een eventueel implementatieplan valt buiten de scope.

Uiteindelijk is er een onderzoeks- en testrapport opgeleverd, met de resultaten van het uitgevoerde onderzoek en de bevindingen van de PoC. Aan het eind wordt een advies gegeven als onderdeel van zowel het testrapport, als deze afstudeerscriptie.

4. Research

"Research is to see what everybody else has seen, and to think what nobody else has thought"

- Albert Szent-Györgyi[II]

4.1. Inleiding

Dit project start met een onderzoek naar de mogelijkheden van de verschillende vormen van VPN die tegenwoordig beschikbaar zijn. Op het eerste gezicht lijkt dit een standaard opdracht, waar een standaard onderzoek voldoende bij is. Er zijn echter problemen die het complexer maken dan verwacht. Deze problemen hebben betrekking op het citaat hierboven.

Aan het begin van het onderzoek werd al snel duidelijk dat de complexe eisen een probleem gingen worden bij het vinden van een oplossing. Een VPN is bedoeld om toegang te krijgen tot het eindpunt en het netwerk daarachter. Maar eigenlijk was het de bedoeling precies de omgekeerde toegang te bereiken; vanuit het eindpunt toegang krijgen tot het netwerk achter het beginpunt. Hierdoor kwam al in de eerste paar weken van het onderzoek naar voren dat dit geen standaard oplossing kon worden en kwam zelfs de gedachte op dat het beoogde ideaal nog nooit eerder was uitgevoerd. Tijdens het onderzoek heeft bovenstaande citaat gediend als inspiratie, om eens *anders* te kijken naar bestaande oplossingen en mogelijkheden. Dat om de mogelijkheid te onderzoeken bestaande oplossingen te gebruiken, op een heel andere manier dan oorspronkelijk bedoeld.

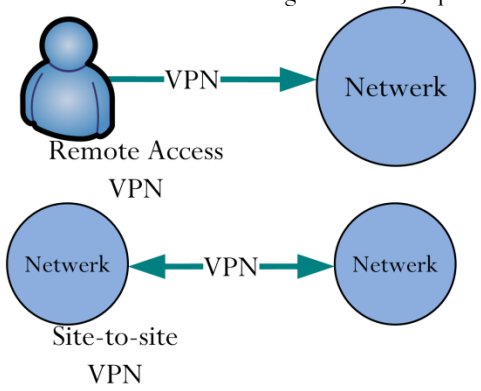
4.2. Oriënteren

Om de verschillende methodes te begrijpen en de mogelijkheden te kunnen bepalen was het noodzakelijk te beginnen met een oriëntatie. VPN maakt gebruik van veel verschillende technieken op het gebied van verbindingsinitiatie, beveiliging, tunnels en datatransmissie. De oriëntatie over VPN, netwerken, componenten en protocollen heeft bijgedragen aan het begrip van mogelijke VPN oplossingen en de verschillen tussen oplossingen van verschillende fabrikanten. Tijdens de oriëntatie werd er zoveel mogelijk informatie verzameld door middel van een (kleine) literatuurstudie.

Een belangrijke insteek bij de oriëntatie: alle technieken, protocollen, etc. werden nog niet beoordeeld op bruikbaarheid voor een oplossing. Er werd geen rekening gehouden met eventuele voorkennis, al bekende eisen of wensen, en/of andere invloeden. Dit heeft twee belangrijk redenen: als eerste is de voorkennis niet compleet genoeg om bij voorbaat technieken, protocollen en andere opties uit te sluiten. Ten tweede verandert de technologie tegenwoordig zo snel, dat het belangrijk is alle opties met een frisse blik te benaderen. Voorkennis kon immers alweer verouderd zijn.

Uit de oriëntatie kwam een beter begrip van VPN en de technieken die ermee gemoeid zijn voort. Belangrijke lering is dat er veel verschillende vormen van VPN zijn en veel verschillende technieken die worden gebruikt.

Globaal is VPN in te delen in twee verschillende architecturen: remote access (of client-server) en site-to-site. De basis van een remote access VPN bestaat uit een gebruiker, die verbinding maakt richting een netwerk om daar toegang te krijgen tot data. Bij een site-to-site VPN wordt de verbinding gemaakt tussen twee netwerken, waarbij beide netwerken voor elkaar beschikbaar zijn (zie figuur 2). Beide architecturen hebben verschillende varianten die gebaseerd zijn op het basisprincipe.



Figuur 2: Remote access en site-to-site VPN

4.3. Eisen en wensen

De volgende stap in het onderzoek was het opstellen van de lijst met eisen en wensen van de betrokken afdelingen, genoemd in hoofdstuk 3.3.

Om een overzichtelijke lijst op te stellen, die de benodigde en gewenste eigenschappen van de oplossing goed weergeeft is gebruik gemaakt van de **M**o**SC**o**W** methode. Deze maakt gebruik van een indeling in vier categorieën: **M**ust have, **S**hould have, **C**ould have en **W**on't have. Bij dit project is gebruik gemaakt van de eerste drie. De laatste categorie (won't have) is bedoeld om toekomstige functionaliteiten te benoemen, die nu nog niet interessant/belangrijk genoeg zijn om rekening mee te houden. Bij dit project is dat echter niet mogelijk, omdat er gebruik wordt gemaakt van bestaande technieken. Het was niet de intentie van het afstudeerproject een nieuwe techniek te ontwikkelen, waarbij op een later moment functionaliteit kan worden toegevoegd.

Tijdens het opstellen van de lijst was het belangrijk bij functionaliteiten een duidelijk onderscheid te maken tussen een eis (must have), zeer gewenst (should have) en gewenst (could have). Ook was het belangrijk om het aantal daadwerkelijke eisen zo veel mogelijk te beperken, en (indien mogelijk) de gewenste functionaliteit als *should have* toe te voegen aan de lijst om de kans op een mogelijke oplossing te vergroten. Op sommige punten was het echter niet mogelijk concessies te doen.

Om duidelijk te krijgen wat er benodigd was in de nieuwe oplossing is er veelvuldig overleg geweest met de verschillende afdelingen, zowel via de mail als in vergaderingen. Hier zijn vooral de afdeling IT Infra./Projects en de afdeling Control Support bij betrokken geweest om de lijst mee op te stellen. De afdeling Service DPP maakt maar sporadisch gebruik van de beschikbare VPN, en had daarom alleen wensen op het gebied van gebruiksgemak.

Na het inventariseren en prioriteren van alle punten die uit overleg naar voren zijn gekomen, kwam de volgende lijst met eisen tot stand:

- **Vanderlande controlled**
  Waarmee wordt bedoeld dat de oplossing beheerd moet kunnen worden door VI.
- **Directe toegang tot alle clients**
  Het moet mogelijk zijn om alle materialen van VI bij de klant direct te benaderen, ook Programmable Logic Controllers (PLC)*.
- **Uitgaande verbinding vanuit klantoptiek**
  De verbinding moet vanuit de klant worden geïnitieerd.
- **Goede schaalbaarheid**
  De verwachte groei van het aantal klanten dat door VI beheerd wordt moet opgevangen kunnen worden met de nieuwe oplossing.
- **Goede veiligheid**
  De data moet beveiligd en versleuteld verstuurd worden en ook de integriteit van de data moet worden gegarandeerd.

Een belangrijke opmerking is de aanwezigheid van PLC's bij de klant, die direct benaderbaar moeten zijn vanuit VI. PLC's zijn onderdelen van automatische systemen, die vergeleken kunnen worden met primitieve robots. Een PLC heeft maar beperkte functionaliteiten op het gebied van IP connectiviteit. Een PLC kan geen gebruik maken van protocollen als het Remote Desktop Protocol (RDP)* of technieken als "Hulp of afstand" van Microsoft. Toch moet er een directe verbinding staan om op afstand een PLC te kunnen besturen (met gebruik van speciale software). Deze directe verbinding kan gerealiseerd worden met behulp van VPN.

Daarnaast zijn er nog meer wensen kenbaar gemaakt, die niet als eis op de lijst staan. De volledige lijst met alle eisen en deze wensen is terug te vinden als onderdeel van de oplossingsmatrix (Bijlage III).

Over het geheel genomen werd ook de "acceptatiegraad" van de oplossing meegenomen. Hiermee wordt bedoeld: is de oplossing acceptabel voor een klant? Dit is mede afhankelijk van de benodigde apparatuur, of veranderingen aan de bestaande infrastructuur, aan de kant van de klant. Ook de kosten en de benodigde tijd voor implementatie spelen een rol. Bij het opstellen van de eisen is rekening gehouden met de klant. Het duidelijkste voorbeeld hiervan is zichtbaar bij de initiatie: deze moet vanuit de klant komen in plaats van VI. Verwacht wordt namelijk dat klanten eerder een uitgaande dan inkomende verbinding zullen toestaan. Ook bij de eisen wat betreft veiligheid en beschikbaarheid is rekening gehouden met het commentaar van zowel voormalige en huidige klanten, als mogelijke wensen van nieuwe klanten.

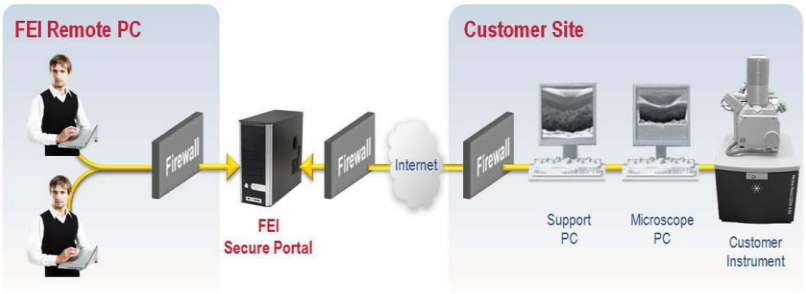
4.4. Inventariseren

Voordat er oplossingen uit het onderzoek naar voren konden komen, moest er gekeken worden naar een grote verscheidenheid aan opties. Deze mogelijkheden werden op basis van de lijst met eisen en wensen beoordeeld. Om een goed beeld te krijgen is gezocht naar oplossingen van verschillende merken, leveranciers en types.

Zoals al eerder is aangegeven, kwam bij de inventarisatie van de mogelijkheden al snel aan het licht dat de eisen en dan voornamelijk de combinatie *directe toegang* met een *uitgaande verbinding vanuit de klant*, zorgden voor een moeilijke situatie. De eerst onderzochte oplossingen vielen vrijwel meteen af op basis van alleen deze twee eisen. Overwogen opties waren bijvoorbeeld Cisco WebEx, Teamviewer, NetSupport Manager en de Microsoft Unified Access Gateway in combinatie met Secure Socket Layer VPN (SSL VPN)*. Deze hebben echter meerdere problemen. De Microsoft oplossing maakt gebruik van de client-server architectuur. Bij deze optie zou het betekenen dat de client aan de VI kant staat en er dus een inkomende verbinding is vanuit klantoptiek, in plaats van een uitgaande verbinding. Daarnaast wordt er gebruik gemaakt van Microsoft producten en niet van Cisco producten, waardoor er problemen kunnen ontstaan met de huidige infrastructuur die uit Cisco apparatuur bestaat.

Cisco WebEx, Teamviewer en NetSupport Manager zijn softwarematige oplossingen voor VPN. Het principe achter deze opties is het opzetten van een soort RDP-sessie waarmee de te beheren computer wordt overgenomen. Zoals eerder vermeldt, is dit door de aanwezigheid van PLC's in de klantnetwerken niet mogelijk. Op basis van deze bevindingen is besloten alle soortgelijke softwarematige opties niet meer te onderzoeken, vanwege de aanname dat al deze mogelijkheden met soortgelijke problemen kampen.

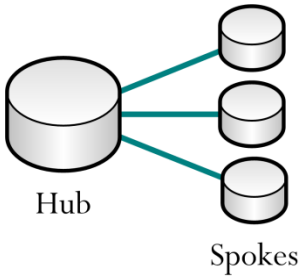
Een laatste oplossing die onderzocht is in dit deel van het onderzoek is Remote Access Program for Interactive Diagnostics (RAPID)*. Deze oplossing wordt gebruikt bij het bedrijf FEI, een partner van VI. FEI is gevestigd in Eindhoven en gespecialiseerd in elektronische microscopen. Tijdens een bezoek van VI medewerkers van de afdeling IT aan FEI in december 2009, kwam naar voren dat FEI deze oplossing gebruikt voor het beheren van apparatuur die zij bij klanten plaatsen. Naar aanleiding hiervan is tijdens het onderzoek contact gezocht met FEI, met het verzoek informatie te sturen over deze oplossing. Uit de ontvangen informatie bleek echter dat de oplossing gebruik maakt van een computer in het netwerk van de klant waar eerst naartoe verbonden moet worden. Daarna kan pas een verbinding worden gelegd naar de apparatuur (zie figuur 3). Omdat dit niet voldoet aan de eis met betrekking tot directe toegang is deze oplossing afgewezen.



Figuur 3: RAPID oplossing[4]

Om toch tot een oplossing te komen, is besloten om het zoekgebied te verbreden en ook de meer onorthodoxe oplossingen te onderzoeken. Hierbij kwam onder andere een mogelijkheid aan het licht die gebruikt maakt van Network Address Translation (NAT)* trucs, om het VPN dataverkeer in goede banen te leiden. Deze optie was echter ineffectief, voornamelijk door de grote hoeveelheid benodigde configuratie en de bemoeilijking van het dagelijks beheer. Aangezien de oplossing gebruikt gaat worden voor ongeveer 120 klanten, met een verwachte groei naar zeker 150, is het niet reëel om veel handmatige configuratie nodig te hebben voor de oplossing. Ook is deze oplossing gebaseerd op een site-to-site VPN met twee eindpunten. Het eindpunt bij de klant zou lokaal beheerd moeten worden, wat zou betekenen dat de oplossing maar gedeeltelijk door VI beheerd wordt.

Met deze resultaten van het onderzoek in het achterhoofd, werd het belangrijk te bepalen hoe er verder gezocht kon worden naar een goede oplossing. Dit kon door op een andere manier te kijken naar de standaard oplossingen en te kijken of met kleine aanpassingen toch een oplossing mogelijk was. Drie opties zijn in dit stadium overwogen: Dynamic Multipoint VPN (DMVPN)* en twee opties gebaseerd op een omgedraaide client-server architectuur.



Figuur 4: DMVPN opstelling

DMVPN is een Cisco techniek, bedoeld om een VPN tunnel op te bouwen vanuit één beginpunt naar twee of meer eindpunten (zie figuur 4). Een soort uitgebreide "hub-spoke" opstelling. Deze optie is overwogen omdat er in principe sprake is van een tunnel met meerdere eindpunten als VI met alle klanten als een geheel benaderd wordt. Ook al zou deze techniek in theorie gebruikt kunnen worden voor de situatie van VI, oorspronkelijk is DMVPN niet bedoeld voor een dergelijke opstelling. Één van de sterke punten van DMVPN is dat de spokes met elkaar kunnen praten, zonder dat een directe verbinding tussen de spokes nodig is. De verbinding loopt dan via de hub. In de situatie van VI is het echter ongewenst als klantnetwerken met elkaar kunnen communiceren. Doordat DMVPN niet op de standaard manier gebruikt kan worden bij VI, is het moeilijk om vooraf een inschatting te maken van de benodigde configuratie en de schaalbaarheid van de techniek.

Een andere gedachte die na overleg naar voren kwam was de omgedraaide client-server constructie. Waarbij de client bij de klant staat en verbinding maakt naar een VPN server bij VI. Dit leverde echter een probleem op. Het netwerk achter de client moest beschikbaar worden gemaakt, wat betekende dat de client ook een routing taak krijgt. Uit het onderzoek kwam naar voren dat hier twee mogelijke manieren voor zijn.

De eerste mogelijkheid was om een machine (met bijvoorbeeld Windows XP Professional als besturingssysteem) in het VI servicenetwerk bij de klant te plaatsen. Een voorbeeld klantnetwerk met bijbehorend VI servicenetwerk is te vinden in bijlage II. De Windows machine kan worden gebruikt als client en router*. Als VPN client zou de Cisco AnyConnect software geïnstalleerd kunnen worden. Deze mogelijkheid voldoet in theorie aan alle eisen, maar het was vooraf niet mogelijk te bepalen of het in de praktijk ook werkt. Hiervoor zou de oplossing verder onderzocht moeten worden in een PoC.

De tweede mogelijkheid was om gebruik te maken van Cisco EasyVPN* in Network Extension Mode (NEM)*, een Cisco techniek om het netwerk achter de VPN client beschikbaar te maken voor de VPN server. Wel moest er een manier gevonden worden om dit te bereiken, zonder hetzelfde probleem te creëren als bij een site-to-site VPN: IP adresseringsproblemen. Hiervoor werd een mogelijkheid aangedragen door een collega. Omdat EasyVPN gebruik maakt van Cisco apparatuur, kan er gebruik worden gemaakt van lokale IP pools. In deze IP pools zitten 1 of meer IP adressen die vooraf gedefinieerd zijn en uniek zijn per klant. Op deze manier zijn de IP adressen van de VPN clients aan de VI kant, uniek voor alle klanten.

4.5. Selectie

Aangezien er maar weinig oplossingen waren die, na het beginnend onderzoek, niet afgewezen waren was het maken van een selectie vrij gemakkelijk. Als eerste stap is er een oplossingsmatrix opgesteld waar alle bekeken oplossingen en alle eisen en wensen in zijn opgenomen. Uit deze matrix is de conclusie getrokken dat er maar drie oplossingen overbleven om te worden overwogen voor de PoC; DMVPN, Omgedraaide client-server met Cisco AnyConnect en Cisco EasyVPN met NEM.

Vanwege de tijd die beschikbaar was voor het project is ervoor gekozen om twee oplossingen te testen in een PoC. Als eerste is er voor gekozen om de Cisco EasyVPN oplossing te testen. Deze was, naar verwachting, gemakkelijker te implementeren dan de andere twee opties en had de grootste kans op succes. Als tweede oplossing om te testen is er gekozen voor de omgedraaide client-server techniek met Cisco AnyConnect. Tussen de twee oplossingen Cisco AnyConnect en DMVPN werd de keuze voornamelijk gebaseerd op de verwachte hoeveelheid configuratie en de kans op succes. Bij de Cisco AnyConnect oplossing was de verwachte configuratie kleiner en gemakkelijker te beheren dan bij DMVPN. Daarnaast maakt Cisco AnyConnect gebruik van de standaard SSL poort (TCP 443), die vaak al naar buiten open staat bij de klant; beveiligde webtoepassingen, zoals Internetbankieren en e-mail, worden ook over deze poort benaderd. DMVPN maakt gebruik van de standaard IPSec poorten, die in veel gevallen specifiek opengezet moeten worden door de klant. DMVPN werd achter de hand gehouden, voor het geval dat beide andere opties niet bleken te werken.

De oplossingsmatrix, waarin de resultaten van het onderzoek zijn verwerkt, is te vinden in bijlage III.

5. Proof of Concept

5.1. Inleiding

Het testen van een gevonden oplossing is in de wereld van IT net zo belangrijk, en misschien wel belangrijker, als het vinden van de oplossing zelf. Zo ook in dit project. Testen was een noodzakelijke stap: er werd gekeken naar oplossingen die op dat moment alleen in theorie onderzocht waren; vooraf kon niet met zekerheid worden gezegd of de gevonden methodes werkten en wat er bij kwam kijken aan configuratie, tijd en/of apparatuur.

Om de uitvoerbaarheid en haalbaarheid van de gekozen oplossingen aan te kunnen tonen is er voor gekozen om een PoC uit te voeren. Dit is een vorm van testen waarbij geprobeerd wordt aan te tonen dat een theorie of concept in de praktijk uitvoerbaar is. Voordat er een PoC kon worden uitgevoerd zijn er twee documenten opgesteld, een ontwerpdocument en een testplan.
In het ontwerpdocument is de verwachte eindopstelling in een "live" omgeving opgesteld. Het netwerkontwerp in dit document is gebruikt om een realistische PoC-omgeving op te kunnen zetten.
In het testplan is uitgelegd welke apparatuur er voor de PoC's zou worden gebruikt en hoe de verbindingen tussen de verschillende componenten lagen. Daarnaast is er een checklist gemaakt, die gebruikt is om de basisopstelling van de PoC's te verifiëren. Het gaat dan om de netwerkverbindingen tussen de onderdelen, zonder dat er gebruik wordt gemaakt van VPN.

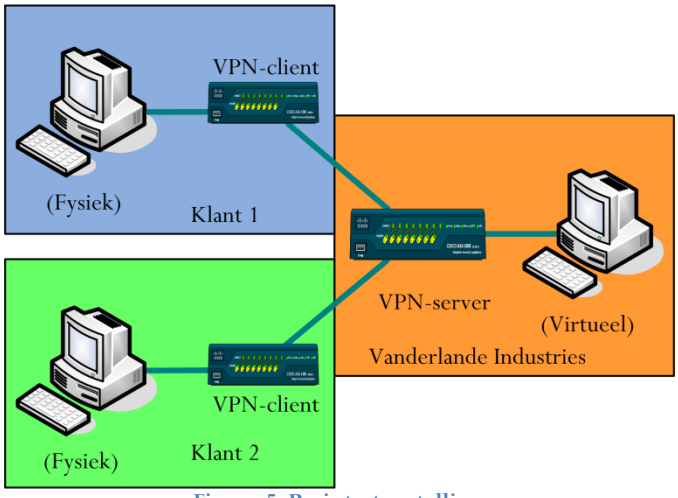
Zoals aangegeven in hoofdstuk 4 is er begonnen met de PoC van de Cisco EasyVPN oplossing en is daarna de PoC uitgevoerd die gebaseerd was op Cisco AnyConnect en SSL VPN.

5.2. Cisco EasyVPN

5.2.1. Testomgeving en apparatuur

Om EasyVPN te kunnen testen waren er verschillende onderdelen nodig; zo moest er een machine zijn die kon fungeren als EasyVPN server en twee machines die konden dienen als EasyVPN client. Om EasyVPN te gebruiken kan er gewerkt worden met Cisco routers of met Cisco Adaptive Security Appliances (ASA's). Een ASA is een apparaat dat de functies heeft van zowel een firewall, als een VPN server. Er is voor gekozen om te werken met ASA's om drie redenen: de ASA's waren beschikbaar om mee te testen, ze hebben meer mogelijkheden wat betreft troubleshooting en hebben de toegevoegde waarde van firewall functionaliteit. De twee eerstgenoemde redenen zijn belangrijk voor tijdens het testen. De derde reden is van belang voor het uiteindelijke resultaat; een firewall verhoogd de beveiliging van de oplossing. Er zijn verschillende modellen ASA's beschikbaar, van de 5505 tot de 5580. In de testomgeving is gebruik gemaakt van het model 5505. Dit is de enige variant die zowel als EasyVPN server en als client gebruikt kan worden. Andere ASA modellen kunnen alleen als EasyVPN server gebruikt worden.

In de testopstelling is ook gebruik gemaakt van drie Windows XP Professional machines die clients in het netwerk simuleren. Twee van deze draaiden als fysieke computers, de clients in de klantnetwerken. De client aan de VI zijde draaide virtueel op de bestaande VMware servers. Deze VMware servers zijn onderdeel van het interne netwerk van VI en worden momenteel al in productie gebruikt om VPN verbindingen op te zetten naar bestaande klanten. De uiteindelijke opzet van de testomgeving zag er uit zoals weergegeven in figuur 5:



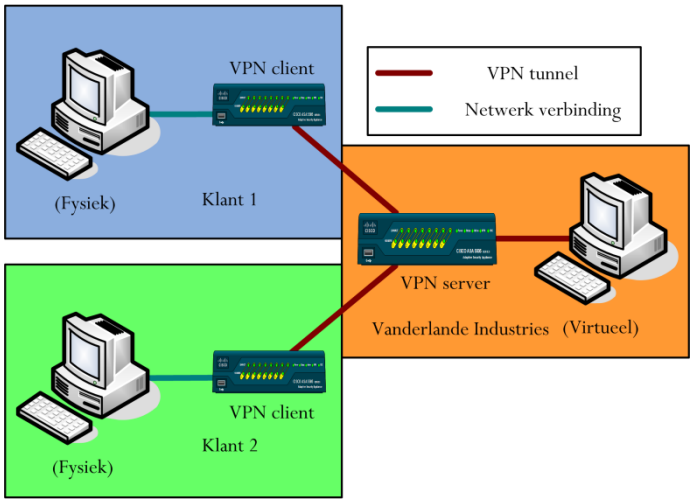
Figuur 5: Basis testopstelling

Deze testopstelling is een geminimaliseerde reflectie van de huidige omgeving. In de echte situatie zijn deze netwerken uitgebreider en bevatten ze meer componenten. Voor het testen is dit verder niet relevant, aangezien met drie clients de benodigde tests kunnen worden uitgevoerd. Het belangrijkste onderdeel van deze opstelling is het testen met twee klanten in plaats van één; dit wordt verder uitgelegd in paragraaf 5.2.3.

5.2.2. EasyVPN en VPN tunnels

Nadat met behulp van de checklist uit het testplan alle verbindingen waren geverifieerd, kon er begonnen worden met de initiële configuratie van EasyVPN. Zoals eerder vermeld kan EasyVPN in zowel client als server modus gedraaid worden. Hierbij maakt de client verbinding richting de server. Om deze reden is begonnen met het configureren van de EasyVPN server. De server waar verbinding naar wordt gemaakt moet immers beschikbaar zijn tijdens het configureren van de client.

Er moesten twee type clients verbinding kunnen maken richting de VPN server: de ASA 5505 in EasyVPN clientmodus die vanaf de klant verbinding maakt en de support engineer die verbinding maakt vanaf de virtuele machines met behulp van Cisco VPN software. Voor de duidelijkheid: de EasyVPN client zal worden aangeduid met “VPN client”, de VPN software met “softwareclient”.
Op de VPN server moet geconfigureerd worden hoe er omgegaan dient te worden met clients die verbinding proberen te maken met de server. Dit wordt gedaan aan de hand van het Internet Security Association en Key Management Protocol (ISAKMP). Dit protocol zorgt voor de benodigde instellingen die te maken hebben met beveiliging en encryptie. Er wordt gekeken naar de toegestane encryptie- en beveiligingsmethodes en naar de mogelijkheden van zowel de client als de server. Daarnaast moest er per client een VPN groep en groepspolicy* worden geconfigureerd. Deze bepalen samen welke instellingen de VPN client ontvangt. Voorbeelden hiervan zijn het IP adres dat de client moet gebruiken (bij softwareclients), welke netwerken onderdeel zijn van de VPN tunnel en welke ISAKMP policy voor deze client geldt. Een belangrijke instelling voor de EasyVPN clients, die in de groepspolicy vermeld staat, is dat er gebruik gemaakt moet worden van de NEM techniek. Na het toepassen van deze instellingen kan er verbinding gemaakt worden vanuit de VPN client en de softwareclient. Uiteindelijk levert dit de situatie op zoals weergegeven in figuur 6:



Figuur 6: Testopstelling met VPN

Om te begrijpen hoe EasyVPN kan worden gebruikt bij VI, is het belangrijk aan te stippen hoe IP adressen worden toegekend aan de softwareclients. Hier komen de lokale IP pools naar voren die in hoofdstuk 4 kort vermeld stonden. Deze IP pools zijn gedefinieerd op de VPN server en bevatten elk vier IP adressen. Deze adressen zijn per klant uniek. Zo heeft bijvoorbeeld klant 1 de adressen 10.5.0.1 t/m 10.5.0.4 en klant 2 10.5.0.5 t/m 10.5.0.8. De softwareclient krijgt één IP uit de pool van de klant, waarvan hij de verbinding opstart.

5.2.3. NEM en het twee klanten probleem

NEM wordt gebruikt om het servicenetwerk van VI bij de klant te bereiken zonder tussenstap. Dit servicenetwerk bevat alle apparatuur van VI die bij de klant staat en waar support voor geleverd wordt. Door gebruik te maken van NEM wordt het mogelijk directe toegang te verkrijgen tot machines en apparatuur. Hierdoor kunnen problemen van klanten op afstand verholpen worden. De VPN client krijgt van de VPN server informatie over het gebruik van NEM en het netwerk dat

toegankelijk gemaakt moet worden, op basis van de VPN groep waar de verbinding mee wordt opgezet. NEM is echter maar een gedeelte dat nodig is om de oplossing werkend te krijgen. EasyVPN gecombineerd met NEM maakt het mogelijk een soort site-to-site VPN te bouwen met een client-server architectuur. Hierdoor wordt echter het grootste probleem van site-to-site VPN's niet veranderd: twee klanten die dezelfde IP range gebruiken voor het servicenetwerk en support dienen te ontvangen op apparatuur in dit netwerk. VI heeft geen zeggenschap over de gebruikte IP range voor het servicenetwerk; er kan dus niet gegarandeerd worden dat de range uniek is, gekeken naar alle klanten van VI. Meestal wordt hier door de klant een range voor aangewezen, gebaseerd op de indeling van hun netwerk. Aangezien VI aan een groot aantal klanten support levert via VPN, kan het voorkomen dat de IP range voor twee klanten gelijk is. En hier zit een probleem: als de VPN server twee servicenetwerken kent waarin een machine staat met bijvoorbeeld het IP adres 172.17.0.1, dan kan de server niet meer bepalen welk van de twee machines wordt bedoeld.

De oplossing hiervoor ligt in de IP pools die worden gebruikt voor de softwareclient. De IP adressen die gereserveerd zijn op de VPN server worden gekoppeld aan een specifieke klant. Hierdoor weet de VPN server dat dataverkeer vanaf één van die IP pools altijd naar de klant moet waar de IP pool aan verbonden is. De link tussen een klant en een IP pool is vastgelegd in een Access Control List (ACL) *. Deze ACL wordt gedefinieerd in de groepspolicy van de VPN client. Een voorbeeld ACL ziet er zo uit (IP 10.5.0.1 (softwareclient) wordt gekoppeld aan het netwerk 172.17.0.0/24 (servicenetwerk)):

```
"Access-list Klant1 extended permit ip 10.5.0.1 255.255.255.255 172.17.0.0
255.255.255.0"
```

Voor klant 1 geldt dat al het dataverkeer van IP 10.5.0.1 altijd naar het servicenetwerk bij klant 1 wordt gestuurd. Ook wanneer er meer klanten zijn waar range 172.17.0.0/24 wordt gebruikt. Dit komt doordat de ACL (in dit geval met de naam "Klant1") gekoppeld is aan de groepspolicy die door de VPN client van klant 1 gebruikt wordt.

5.2.4. Testen met een PLC

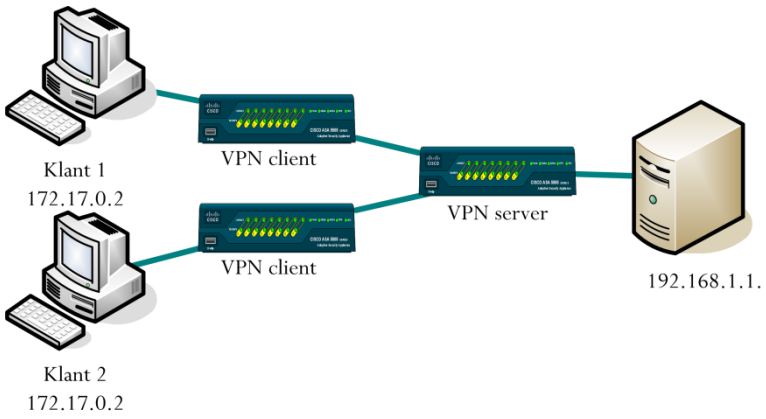
Een belangrijk onderdeel van de systemen die VI bij klanten plaatst zijn PLC's. Deze machines zijn moeilijk van op afstand te beheren door de beperkte verbindingsmogelijkheden. Support engineers bij VI maken gebruik van Siemens software genaamd "Step 7" om support te leveren voor PLC's. Één vereiste voor deze software is echter dat de PLC's direct te benaderen zijn. Om dit te testen is er voor een korte periode een PLC toegevoegd aan het testnetwerk van klant 1. Deze PLC heeft een vast IP adres gekregen, uit de range van klant 1, waarop hij te benaderen moest zijn vanaf de softwareclient. Het testen van de verbinding richting de Windows client was al geslaagd en ook de verbinding naar de PLC kon zonder problemen worden opgezet met de Step 7 software.

Na het testen van deze functionaliteit was het duidelijk dat de EasyVPN oplossing voldeed aan alle eisen. Nu kon er gekeken worden naar *gewenste* functionaliteiten. Eerst moest echter een potentieel probleem, aangekaart door een dochterbedrijf van VI worden onderzocht en opgelost.

5.2.5. Het updateserver probleem

Tijdens het uitvoeren van de tests werd er door een collega van het Duitse dochterbedrijf van VI, LSG, een probleem naar voren gebracht. LSG levert remote support aan klanten via voornamelijk site-to-site VPN's. Tot nu toe zijn daarmee geen problemen ontstaan, omdat LSG een aanzienlijk kleiner aantal klanten support en daarnaast minder IP ranges gebruikt in hun interne netwerk. Door dit beperktere aantal klanten zijn er nog geen conflicten ontstaan tussen IP ranges van klanten en/of LSG.

Één van de diensten die voor LSG belangrijk is, heeft betrekking op de updates voor o.a. Windows en antivirus programma's. Indien er machines in het servicenetwerk staan waarvoor updates noodzakelijk zijn, kan er geregeld worden dat deze updates via de servers van VI (of LSG) binnen worden gehaald. Voor Windows komen deze updates van een zogeheten Windows Server Update Services (WSUS) machine; voor antivirus programma's kan worden gedacht aan McAfee ePolicy Orchestrator (ePo). Het probleem is echter dat er maar één WSUS of ePo server beschikbaar is aan de VI kant. Dit betekent dat deze server voor alle klanten op hetzelfde IP benaderbaar moet zijn waardoor het twee klanten probleem, dat met IP pools was opgelost, weer geldt voor deze servers. De servers krijgen namelijk geen IP toegewezen van de VPN server zoals een client, maar hebben een eigen vast IP adres. Zie figuur 7 ter illustratie:



Figuur 7: Updateserver setup

Als de pc genaamd "Klant 1" een update van de server wil halen, wordt er verbinding gemaakt van 172.17.0.2 naar 192.168.1.1. Op de heenweg gaat dit goed, maar als de VPN server dataverkeer krijgt van 192.168.1.1. naar 172.17.0.2 zijn er twee mogelijke eindbestemmingen (Klant 1 en 2). In paragraaf 5.2.3. is uitgelegd hoe IP pools hiervoor een oplossing bieden, wanneer gebruik wordt gemaakt van (virtuele) softwareclients. Voor de updateserver werkt dit echter niet, aangezien de server een vast IP heeft en niet via VPN verbonden is met de VPN server, maar via het VI netwerk.

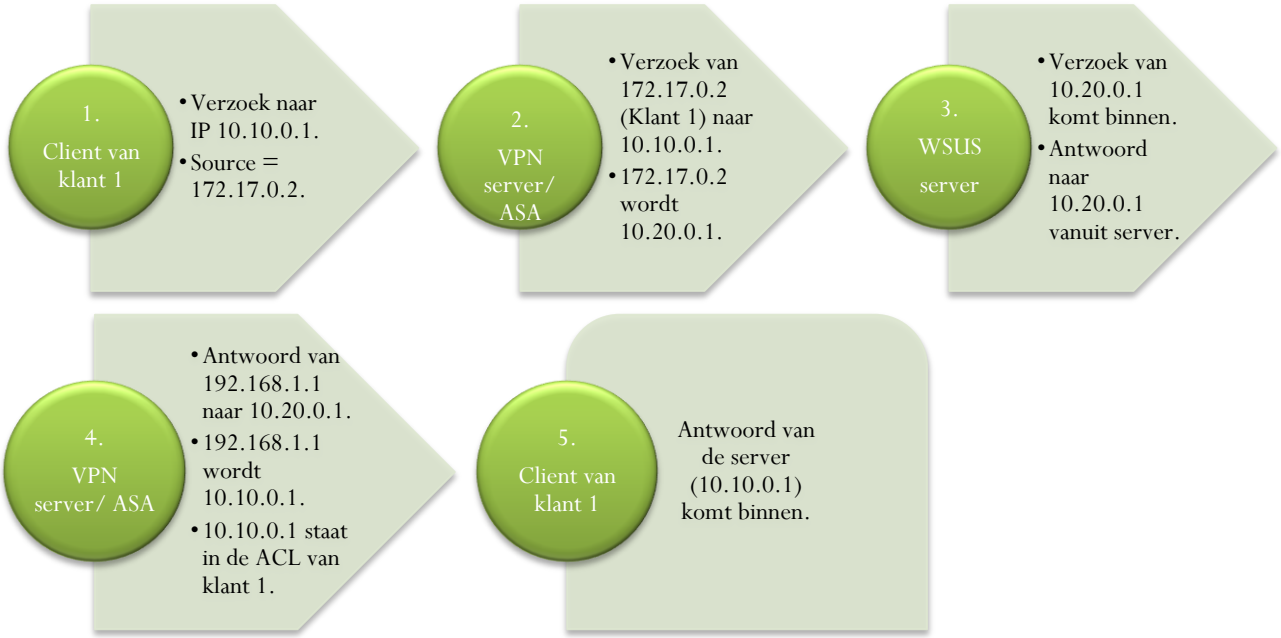
Om dit probleem op te lossen moet er gebruik gemaakt worden van NATting binnen in de VPN server. NAT is al heel kort benoemd in hoofdstuk 4, toen het naar voren kwam als mogelijke oplossing voor de gehele VPN problematiek. Het bleek toen echter inefficiënt om op grote schaal uit te voeren. Voor dit probleem kan NATting echter wel gebruikt worden; het geldt maar voor een beperkt aantal klanten en heeft geen negatief effect op de rest van de EasyVPN oplossing.

NAT is een techniek die gebruikt wordt om een IP adres naar een ander IP adres te vertalen. Meestal gaat het dan om meerdere privé adressen die naar één publiek adres worden vertaald. Dit kan ook gebruikt worden binnenin de VPN server. Door gebruik te maken van een NAT policy kan er gekeken worden naar het beginpunt van het dataverkeer, de "source", en naar het eindpunt, de "destination". Op basis van deze twee gegevens kan het source IP worden vertaald naar een ander IP adres. Wordt dit gedaan in beide richtingen, server naar client dataverkeer en client naar server dataverkeer, dan kan de verbinding gemaakt worden tussen de twee vertaalde IP adressen. Per klant is er dus sprake van twee NAT policies, zie figuur 8:

#	Type	Original			Translated	
		Source	Destination	Service	Interface	Address
DMZ						
1	Static Policy	WSUSserver	10.20.0.1		outside	10.10.0.1
2	Static Policy	WSUSserver	10.20.0.2		outside	10.10.0.2
outside						
1	Static Policy	Klant_1	10.10.0.1		DMZ	10.20.0.1
2	Static Policy	Klant_2	10.10.0.2		DMZ	10.20.0.2

Figuur 8: Voorbeeld NAT policies voor twee klanten

De WSUS server wordt per klant vertaald naar een uniek IP in de 10.10.0.0/24 range. De client bij de klant wordt vertaald naar een IP uit de range 10.20.0.0/24. Vanaf de client en de server wordt dus verbinding gemaakt naar het *vertaalde* IP adres en niet naar het origineel, ook al bestaat dit adres alleen binnen in de VPN server. Om de terugweg goed te laten verlopen, moet het vertaalde IP adres van de server toegevoegd worden aan de ACL voor de klant. Dit is dezelfde ACL die eerder is gedefinieerd als onderdeel van de groepspolicy (zie paragraaf 5.2.3.). Het processchema uit figuur 9 toont aan hoe een verzoek vanuit klant 1 wordt afgehandeld met de NAT policies:



Figuur 9: Processchema clientverzoek

5.2.6. Overige functionaliteiten en wensen

Buiten de eisen zijn er vooraf ook wensen opgesteld. Het gaat hier dan om onderdelen zoals logging, gebruiksgemak en opties om een hoge beschikbaarheid te garanderen. Om alle wensen hier uitgebreid te behandelen vereist teveel technisch inzicht en een uitgebreidere achtergrond van de situatie. Deze informatie staat in het testrapport, bijgevoegd als bijlage IV. De resultaten van de extra onderzochte functionaliteiten/wensen worden alleen beknopt genoemd:

Logging: één van de eerste wensen die onderzocht is, betreft de mogelijkheid tot logging en monitoring van de status van de tunnel. Dit is mogelijk door gebruik te maken van de log meldingen van de ASA's. Hiermee wordt de mogelijkheid tot proactief beheer gecreëerd. Logging op de ASA kan gebruik maken van de syslog server die VI momenteel gebruikt voor servermonitoring, om meldingen naar toe te sturen.

Gebruiksgemak: voor eindgebruikers van VPN binnen VI verandert er weinig voor het dagelijks gebruik. Het beheer krijgt een gemakkelijkere taak, mede door het monitoren en loggen en het hebben van een standaard. Het configureren van ASA's voor nieuwe klanten wordt een simpelere taak, die in minder tijd kan worden volbracht dan bij de huidige oplossingen.

Beschikbaarheid en failover: mogelijkheden voor het redundant uitvoeren van de oplossing zijn beschikbaar voor VI. De VPN server in het netwerk van VI kan redundant worden uitgevoerd, als gebruik wordt gemaakt van de ASA 5510 of hoger. De ASA bij de klant kan niet als failover worden uitgevoerd door beperkingen van de ASA 5505 in combinatie met EasyVPN. Er kunnen echter wel twee ASA's geplaatst worden, waarbij de tweede uitstaat en in geval van nood ingeschakeld kan worden.

Aantal gelijktijdige gebruikers en VPN tunnels: het aantal gebruikers van VPN verbindingen wordt voornamelijk beperkt door het aantal VM's dat tegelijkertijd kan worden gedraaid. Dit is afhankelijk van de VMware servers. Het aantal gebruikers per VPN van één specifieke klant is afhankelijk van de grote van de IP pool. In de testomgeving was dit aantal vier (4 IP's), maar meer is mogelijk. Het aantal mogelijke tunnels (en dus klanten) is afhankelijk van het model ASA aan de VI kant. Het aangeraden model is de ASA 5510, waarbij 250 gelijktijdige tunnels mogelijk zijn. Dit is voldoende voor het huidige aantal klanten en om de verwachte groei op te vangen. Indien nodig zijn er ook duurdere modellen beschikbaar, die 750 of meer gelijktijdige tunnels aan kunnen; een toekomstige upgrade is daardoor mogelijk.

Automatisch opstarten VPN tunnel: het automatische starten van de VPN verbinding is mogelijk met de autoconnect optie op de VPN client. Het wordt aangeraden deze optie aan te zetten zodat ook tijdelijke haperingen in de Internet verbinding geen effect hebben op de tunnel. Indien de klant dit wenst kan echter ook voor manuele verbinding worden gekozen.

Beveiliging: informatiebeveiliging is een belangrijk item in de tegenwoordige IT wereld en is zowel voor (potentiële) klanten als VI belangrijk. Een wens vanuit het beheerteam was betere beveiliging en veiligere vormen van authenticatie. Voor beveiliging van de VPN tunnel en de data worden de sterkste algoritmes, die beschikbaar zijn op de ASA, gebruikt: de 256 bit variant van de Advanced Encryption Standard (AES) en het Secure Hash Algorithm (SHA). Deze zorgen respectievelijk voor data-encryptie en data-integriteit. Voor authenticatie bestaat er bij de ASA de mogelijkheid tot het gebruik van smart cards/tokens* of certificates, om authenticatie veiliger te maken. Het onderzoeken van deze beveiligingsmethodes viel echter buiten de scope van het project.

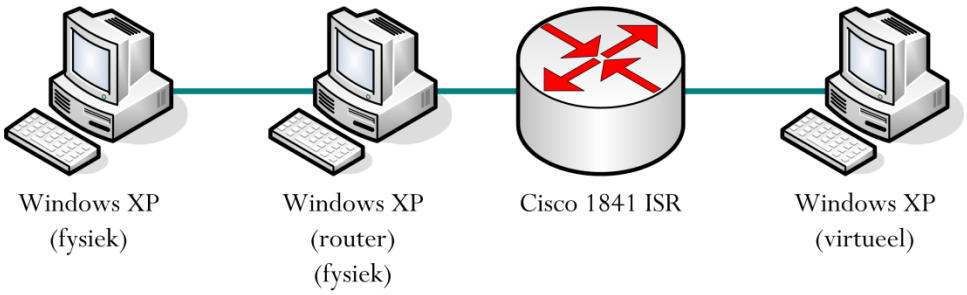
5.3. Cisco AnyConnect en Policy Based Routing (PBR)

De titel van deze paragraaf behoeft wat uitleg; de term PBR is toegevoegd.
Twee soorten dataverkeer zijn belangrijk bij netwerkverbindingen; het dataverkeer op de heenweg en het dataverkeer op de terugweg. Beide soorten dataverkeer moeten de juiste route nemen over het netwerk. Deze route wordt bepaald door de routes op de verschillende routers van het netwerk. Tijdens het onderzoek naar EasyVPN kwam naar voren dat dataverkeer, als het de juiste heenweg had genomen, niet automatisch een goede terugweg kon vinden. Dataverkeer kwam daardoor niet terug bij het beginpunt. PBR kon hiervoor een oplossing bieden, door de terugweg van dataverkeer te bepalen aan de hand van het begin- en eindpunt van het dataverkeer.

5.3.1. Testomgeving en apparatuur

Cisco AnyConnect maakt gebruik van SSL VPN om verbindingen op te zetten. Om echter SSL VPN te gebruiken zijn meer geavanceerde Cisco routers en licenties benodigd dan beschikbaar waren. De keuze is daarom gemaakt om IPSec VPN te gebruiken met de standaard Cisco VPN software die ook bij EasyVPN was gebruikt. Hierdoor hoefde er geen dure apparatuur en/of licenties te worden aangeschaft. De werking van SSL en IPSec VPN komt in zoverre overeen, dat dit geen grote invloed zou hebben op de betrouwbaarheid van het testresultaat. Bij de AnyConnect oplossing is er voor gekozen om te testen met één klant in plaats van twee. Deze keuze is gemaakt om het aantal fysieke machines te beperken. De ongebruikelijke opbouw van de oplossing maakt het testen met één klant ook een betere optie; zodra de oplossing voor één klant functioneert kan er altijd nog een tweede klant worden toegevoegd.

Uiteindelijk werd de testomgeving opgebouwd met twee fysieke machines met als besturingssysteem Windows XP Professional, één Cisco 1841 Integrated Services Router en dezelfde virtuele opstelling die in de EasyVPN oplossing was gebruikt. Één van de twee fysieke Windows machines beschikte over twee netwerkkaarten. De uiteindelijk opbouw van de testomgeving zag er uit zoals weergegeven in figuur 10:



Figuur 10: Testopstelling AnyConnect/PBR

5.3.2. Theorie en gedachtegang

Om een duidelijke achtergrond te geven van de theorie achter de opbouw van deze oplossing, wordt hier in het kort benoemd wat elk onderdeel in the testomgeving voor taak heeft en wat de gedachte hierbij is. Voor de duidelijkheid: de vier componenten worden van links naar rechts behandeld op basis van figuur 10.

Windows XP client (fysiek): deze machine fungeert alleen als client in het nagebootste klantnetwerk. De enige verbinding is die met de Windows router bij de klant. Hierdoor kan de client op effectieve wijze een machine in het klantnetwerk nabootsen.

Windows XP router (fysiek): deze computer heeft twee netwerkkaarten en fungeert als router voor het klantnetwerk. Door met twee netwerkkaarten te werken kan de pc gebruikt worden als router. Vanuit hier wordt ook de VPN tunnel richting de router opgezet met behulp van Cisco VPN client software.

Cisco 1841 ISR: de router die de functie van VPN server op zich neemt en die met behulp van PBR dataverkeer vanaf de virtuele client naar het klantnetwerk stuurt.

Windows XP client (virtueel): een virtuele Windows XP machine die draait op de VMware servers van VI. Maakt gebruik van Cisco VPN client software om een VPN op te zetten naar de Cisco 1841 ISR.

5.3.3. Windows XP als router

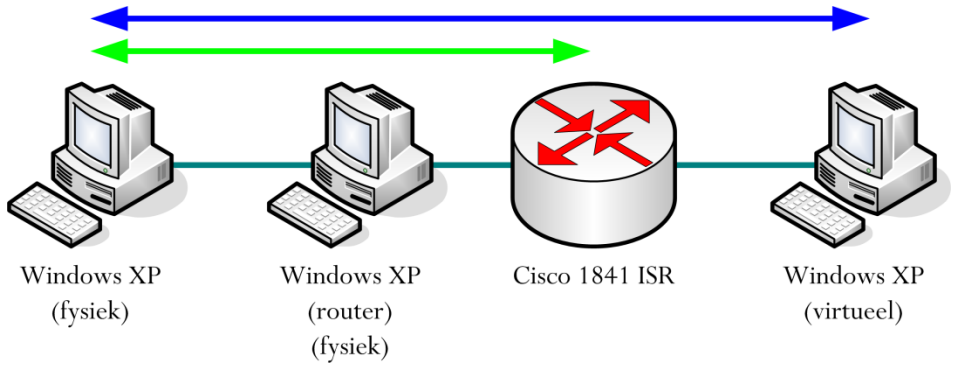
Om het klantnetwerk toegankelijk te maken vanaf de client moet de machine fungeren als router. Dit is bij Windows XP Professional gemakkelijk te realiseren door een register* wijziging toe te passen. Hierbij moet gekeken worden naar de volgende registersleutel:

```
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP\Parameters\IPEnableRouter=1"
```

De standaardwaarde voor de "IPEnableRouter" parameter is 0, wat betekent dat de functie uit staat. Door deze naar 1 te veranderen wordt de router functie van Windows XP geactiveerd. Een router moet echter ook de routes kennen naar de netwerken waar hij mee te maken heeft. In deze testomgeving zijn dit het klantnetwerk en de Cisco router. Omdat de Windows XP machine en de Cisco router aan elkaar gekoppeld zijn, geldt de Cisco router als "default gateway" voor de Windows XP router. Dit betekent dat al het dataverkeer waar geen route voor is automatisch naar de Cisco router wordt gestuurd. Om het klantnetwerk ook beschikbaar te maken moet de volgende route worden toegevoegd op de Windows XP router:

```
"Route ADD 172.17.0.0 MASK 255.255.255.0 172.17.0.1"
```

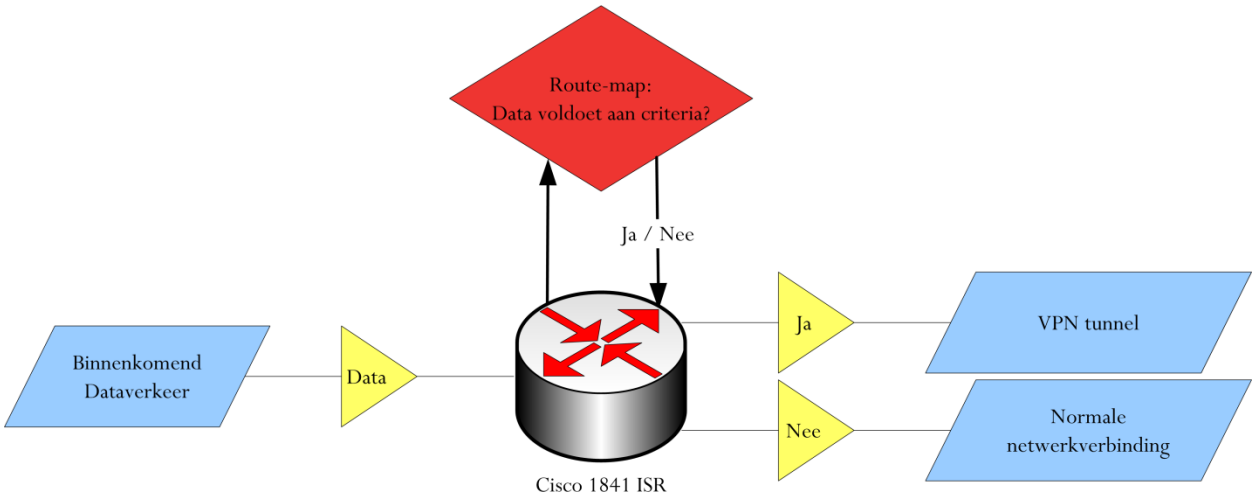
Deze twee wijzigingen zorgen er samen voor, dat het klantnetwerk beschikbaar is vanaf de router (de groene lijn in figuur 11). Na de basisconfiguratie voor de Cisco router volstaat het om ook hier routes toe te voegen naar de verschillende netwerken. Daarna is alle communicatie tussen de verschillende onderdelen mogelijk (zie de blauwe lijn in figuur 11, let wel: dit is nog zonder VPN).



Figuur 11: Testopstelling AnyConnect/PBR na eerste configuratie

5.3.4. Beperkingen van VPN en het einde van de PBR theorie

Nadat de testomgeving werkend was opgesteld moesten de VPN verbindingen en PBR configuratie worden uitgevoerd. Het configureren en opzetten van de VPN tunnels was, door opgedane ervaring met de EasyVPN oplossing, in korte tijd mogelijk. Zoals verwacht, werd het dataverkeer na het opstellen van de VPN verbindingen nog steeds langs en niet door de tunnel tussen de Windows en Cisco router gestuurd. Dit vanwege de routes die waren ingesteld op de routers. Voor VPN moest eerst PBR ingesteld worden, om het dataverkeer door beide tunnels te laten lopen. Via een zogenaamde "route-map" op de Cisco router, wordt bij PBR bepaald waar het dataverkeer naar toe gestuurd wordt. Een route-map kan de route van dataverkeer veranderen op basis van vooraf bepaalde criteria. Hoe dit proces werkt wordt weergegeven in figuur 12:



Figuur 12: Processchema route-map testopstelling

Dataverkeer komt de router binnen en wordt naar het route-map proces gestuurd. De route-map controleert of het dataverkeer voldoet aan de criteria; is de source gelijk aan de virtuele client en de destination gelijk aan de fysieke Windows client? Hieruit komt het antwoord "ja" of "nee". Is het antwoord "ja", dan wordt het dataverkeer de VPN tunnel ingestuurd. Is het antwoord "nee", dan wordt het dataverkeer over de normale verbinding verstuurd, buiten de tunnel om. Dit wordt gedaan door de "next-hop" van het verkeer aan te passen. Een next-hop is de volgende stap die een router kent richting een netwerk/destinaton, maar is niet altijd gelijk aan het eindpunt. Er kunnen meerdere stappen zitten tussen de router en het eindpunt van het dataverkeer. PBR kan deze next-hop veranderen in het IP adres van de VPN interface op de Windows router. De route-map van PBR overruled op deze manier de statische route naar het klantnetwerk, die bij een normale verbinding richting de Windows router wordt gebruikt.

In theorie zou na het implementeren van deze route-map al het dataverkeer vanaf de virtuele client naar de fysieke client door beide VPN tunnels moeten lopen. In de praktijk bleek echter dat het dataverkeer niet verder kwam dan de Cisco router. Na verschillende configuraties en meerdere troubleshooting tools te hebben gebruikt, was de conclusie dat het dataverkeer vanaf de virtuele client niet goed door de Cisco router heenging. Zoals kort in het begin van hoofdstuk 4 besproken, zijn VPN tunnels versleutelde verbindingen. Omdat echter wordt geprobeerd onversleuteld dataverkeer over een VPN tunnel te sturen, wordt dit dataverkeer door de Cisco router gedropt. Het veranderen van de next-hop met behulp van PBR, verandert de destination niet. Deze destination bepaalt wat er met het dataverkeer gebeurd; is de destination gelijk aan het eindpunt van de VPN tunnel, dan wordt het dataverkeer versleuteld; is de destination anders, dan wordt het dataverkeer niet versleuteld. De destination is echter nog steeds gelijk aan de fysieke Windows client en niet aan het eindpunt van de VPN tunnel.

Voor de AnyConnect/PBR oplossing betekende dit dat de theorie niet in de praktijk uitvoerbaar bleek. Zonder gebruik te maken van PBR kon het twee klanten probleem niet worden opgelost, wat betekende dat directe toegang tot alle VI machines niet in alle gevallen mogelijk zou zijn. Aangezien dit als eis was gedefinieerd, was verder testen van de oplossing niet meer noodzakelijk. Om echter meer inzicht te krijgen in de werking van VPN en de precieze oorzaak achter dit testresultaat is op dat moment besloten nog een extra test uit te voeren. Dit keer met gebruik van een ASA in plaats van de Cisco router. Een ASA kan geen PBR gebruiken, maar of het dataverkeer via een route-map of vaste route gerouteerd wordt is niet van belang. De destination van het dataverkeer blijft namelijk nog steeds de fysieke client en niet het VPN eindpunt, ook bij statische routering. Een ASA beschikt echter over meer mogelijkheden om het dataverkeer te monitoren en traceren. Hierdoor kon er onderzocht worden waarom het dataverkeer gedropt werd en op welk moment. Het resultaat van deze test was een bevestiging van de, na het testen met de Cisco router, getrokken conclusie; het dataverkeer werd niet versleuteld en door de ASA aangemerkt als "IPSec spoof". Deze melding betekent dat gewoon dataverkeer zich voordoet als VPN dataverkeer (versleuteld dataverkeer). Deze melding komt nog voordat het dataverkeer de VPN tunnel in gaat, wat verklaart waarom het dataverkeer al op de Cisco router wordt gedropt.

Op basis van deze bevindingen werd besloten niet meer verder te testen met de AnyConnect/PBR oplossing en de testfase af te ronden.

5.4. DMVPN

De DMVPN oplossing is tijdens het onderzoek even aan bod geweest als mogelijke derde oplossing. Na het afronden van de AnyConnect/PBR tests is kort overwogen om ook DMVPN nog te testen. Er is besloten dit niet meer te doen vanwege drie hoofdredenen:
Ten eerste was het zeer waarschijnlijk dat de DMVPN oplossing tegen soortgelijke problemen aan ging lopen als de AnyConnect/PBR oplossing, wanneer gekeken wordt naar het twee klanten probleem.
Ten tweede was de overgebleven tijd niet voldoende om de behaalde resultaten van de twee uitgevoerde PoC's goed te documenteren en daarnaast de DMVPN oplossing, waar van verwacht werd dat deze erg arbeidsintensief zou zijn, op een goede manier te testen.
Ten derde was de benodigde apparatuur niet beschikbaar, aangezien voor de DMVPN oplossing minimaal twee, en eigenlijk drie, routers benodigd waren.

6. Conclusie

Het doel van dit afstudeerproject was het onderzoeken van nieuwe oplossingen voor remote support geleverd door VI, waarbij deze support via VPN uitgevoerd wordt. Dit doel is uitgewerkt door het uitvoeren van een onderzoek en twee PoC's. Wat overblijft is de vraag waar het onderzoek en de PoC's toe hebben geleid.

Een onderzoek naar nieuwe methodes of oplossingen heeft (vrijwel) altijd één van de volgende twee uitkomsten: "positief", wat wil zeggen dat er één of meerdere goede nieuwe oplossingen bestaan of "negatief", wat betekent dat er geen betere mogelijkheid beschikbaar is. Dit project vormde hierop een uitzondering, omdat er twee oplossingen zijn onderzocht. Één resultaat was positief en één resultaat negatief.

Middels een PoC is aangetoond dat de Cisco EasyVPN techniek een oplossing vormt voor vrijwel alle problemen die momenteel bestaan bij het leveren van remote support. Door gebruik te maken van de NEM-modus is het mogelijk één oplossing te gebruiken in vrijwel alle gevallen; EasyVPN is grotendeels onafhankelijk van de situatie bij een klant. Verder heeft EasyVPN verschillende voordelen ten opzichte van de huidige oplossingen; zo verandert er vrijwel niets aan de werkwijze voor de support engineers, waardoor er geen leercurve is. Tevens kan er een betere standaardisatie worden bereikt, doordat voor alle klanten die gebruik maken van EasyVPN de verbinding op dezelfde wijze wordt opgezet. Ook wordt beveiliging en authenticatie in alle gevallen toegepast en zijn er mogelijkheden voor logging en monitoring. EasyVPN kan voor VI een oplossing bieden voor alle huidige problematiek met betrekking tot VPN's.

Daarnaast is via een tweede PoC aangetoond dat de PBR techniek niet gebruikt kan worden om, samen met SSL VPN, de problemen van VI op te lossen. Dit betekent dat er geen simpele manier is om van SSL VPN gebruik te maken in de situatie van VI en het (nog) niet mogelijk is om een oplossing te implementeren die van een standaard poort op de firewall gebruik maakt.

In het kort heeft dit afstudeerproject een onderzoek opgeleverd met informatie over de huidige vormen en mogelijkheden met betrekking tot VPN. De eerste PoC heeft geleid tot een werkende en bruikbare oplossing voor remote support. De tweede PoC heeft geleid tot een beter inzicht in de werking van VPN en routering, en de mogelijkheden van PBR. Deze kennis kan in de toekomst in andere situaties worden benut.

7. Advies

Een onderzoek laten doen naar mogelijkheden om problemen binnen een bedrijf op te lossen is een goede en actieve manier om te streven naar verbeteringen. Er moet echter wel "iets" gedaan worden met de resultaten van het uitgevoerde onderzoek. Gekeken naar de resultaten van het onderzoek en de tests, levert EasyVPN een goede oplossing voor de VPN problematiek binnen VI. Maar om EasyVPN te implementeren zijn er verschillende vervolgstappen, waar over nagedacht moet worden.

Om EasyVPN te kunnen gebruiken binnen VI zal er een project opgestart moeten worden om de implementatie te plannen en uitvoeren. Dit zal moeten gebeuren met goedkeuring van het management. Bij dit implementatieproject kunnen benodigde hardware, software en overige zaken worden gedefinieerd en in detail uitgewerkt (een voorzichtige schatting van de kosten en benodigde projecturen/hardware is onderdeel van het testrapport, zie bijlage IV). Ook kan er gekeken worden hoe EasyVPN in fases geïntroduceerd kan worden, bijvoorbeeld door het eerst op één of meerdere klanten in de praktijk uit te testen. Hiermee kunnen eventuele "kinderziektes" in een later stadium worden voorkomen.

Ook migratie van de huidige klanten naar EasyVPN zal goed doordacht moeten worden aangepakt. Veel klanten zullen moeilijk te overtuigen zijn de investering in EasyVPN te maken, zeker als de huidige oplossing goed functioneert. De klant zou echter overtuigd kunnen worden door de voordelen van EasyVPN, ten opzichte van de huidige oplossingen, te benadrukken. Hierbij kan gedacht worden aan de sterkere beveiligingsopties en de mogelijkheid tot monitoring en logging om proactief problemen met de verbinding op te lossen.

Een laatste belangrijk punt is het beleid binnen VI. Er is een algemeen beleid nodig waar in staat dat EasyVPN gebruikt gaat worden als VPN oplossing voor remote support. Dit beleid moet gelden voor alle onderdelen, ook dochterbedrijven zoals LSG, die tot nu toe vrijwel altijd zelf beslissen hoe remote support wordt ingericht voor hun klanten. Daarnaast moet er tijdens gesprekken met de klant in de verkoopfase al gekeken worden naar remote support en de mogelijkheid die VI daarvoor biedt. In de huidige situatie wordt de IT afdeling pas laat betrokken bij het verkoopproces en moet men zich houden aan de afspraken tussen verkoper en klant. Deze verkopers hebben echter niet voldoende kennis van IT gerelateerde zaken, waardoor soms beloftes worden gemaakt die niet nagekomen kunnen worden. Door de IT afdeling bij de verkoopfase te betrekken kunnen duidelijke afspraken worden gemaakt over hoe VI, remote support bij de klant gaat inrichten. Door de sterke punten te benadrukken kan de klant duidelijk gemaakt worden waarom EasyVPN hiervoor wordt voorgesteld door VI. Alleen in uitzonderingsgevallen zou dan afgeweken kunnen worden van de EasyVPN standaard (bijvoorbeeld voor bepaalde vliegvelden, waar geen (externe) verbindingen naar buiten of binnen worden toegestaan).

Tijdens het lezen van dit rapport en de bijgevoegde documentatie heeft u informatie gekregen over de werking en voordelen van EasyVPN en over VPN oplossingen voor remote support in het algemeen. U heeft hiermee de kennis gekregen die nodig is om een besluit te kunnen nemen over het implementeren van EasyVPN en de verdere vervolgstappen. Immers:

"Nobody can give you wiser advice than yourself"

- Marcus Tullius Cicero[III]

Evaluatie

Tijdens het gesprek bij VI in december 2009, had ik de keuze uit verschillende opdrachten. De inhoud van de opdracht "remote support VPN", was pas een klein uurtje eerder bedacht door Marcel en Maurice op de terugweg van Eindhoven naar Veghel. En eigenlijk sprak de opdracht mij meteen aan. Ik wist echter wel dat mijn kennis van netwerken niet heel uitgebreid was en mijn kennis van VPN nog minder. In het begin was ik bezorgd dat dit een probleem op zou kunnen leveren, maar door vanaf het begin af aan hard te werken en vragen te stellen als ik iets niet snapte, is het uitstekend verlopen. Als ik terugblik op de afgelopen afstudeerperiode dan heb ik, mede door goede begeleiding, veel kennis en ervaring opgedaan. Zoveel zelfs dat er rond de 15de week door Marcel werd gezegd: "Jij weet ondertussen meer van VPN af dan ik". Ook al was dit schromelijk overdreven, er zat (denk ik) wel een kern van waarheid in: het verschil tussen mijn kennis over netwerken en VPN in het begin en op het eind van mijn stage is erg groot.

Naast kennis over het onderwerp heb ik tijdens mijn afstudeerperiode nog veel meer geleerd. Daarbij denk ik onder meer aan het schrijven van duidelijke en informatieve documentatie; het belang van het goed documenteren van negatieve resultaten; aan het duidelijk kunnen uitleggen van behaalde resultaten (vooral aan mensen met minder technische kennis) en aan het uitvoeren van een onderzoek met daarbij de gehele organisatie in het achterhoofd en niet één of een paar afdelingen.

Als ik mijn 3de jaars stage vergelijk met mijn afstudeerstage dan er is een duidelijke groei waarneembaar. Mijn 3de jaars stage was een soortgelijke opdracht (onderzoek naar Microsoft SCOM). De aanpak die ik echter voor mijn afstuderen heb gebruikt, was veel beter georganiseerd en beter gepland. Ook heb ik vanaf het begin hard getrokken aan de opdracht, wat er voor heeft gezorgd dat ik vrijwel de hele afstudeerperiode 2-4 weken heb voorgelopen op de planning. Daarnaast heb ik veel meer initiatief getoond door veel vragen te stellen, zelf met uitbreidingen aan de opdracht te komen, goed aan te geven waar mijn grenzen qua tijd en mogelijkheden lagen en interesse te tonen in collegae, de afdeling en VI.

Toen er een paar weken van mijn afstudeerperiode voorbij waren, begon het mij op te vallen dat iedereen alleen met zijn eigen taken bezig was. Omdat alle medewerkers op de afdeling hun eigen vakgebied hebben, kon ik als stagiair maar moeilijk bepalen met welke projecten en vragen iedereen bezig was. Iets wat ik persoonlijk als heel jammer ervoer, aangezien ik graag betrokken wilde zijn bij het bedrijf. Ik heb dit aangekaart bij mijn beide begeleiders en gevraagd of hier een oplossing voor was. Uiteindelijk ben ik bij het afdelingsoverleg betrokken, wat iedere paar weken wordt gehouden. Hierdoor kreeg ik goed mee wat er op de afdeling gebeurde en wat de verschillende huidige projecten waren. Ik heb hier veel van geleerd, met name wat betreft projectaanpak en problemen die zich kunnen voordoen. Ook heeft Maurice geregeld dat de stagiaires van de afdelingen IT Infra./Projects en IT Infrastructure een rondleiding kregen door het bagagesysteem van Schiphol. Een heel leerzame en leuke ervaring.

Uiteindelijk kijk ik zeer positief terug op mijn afstudeerperiode bij VI. Ik heb al mijn doelen kunnen bereiken; het vergaren van kennis, het leren kennen van het bedrijf en de collegae, het opdoen van ervaring met zowel de technische, als organisatorische kant van de opdracht en het uitvoeren van een goede PoC met betrouwbare en nuttige resultaten. Over al deze resultaten en over deze scriptie, ben ik dan ook zeer tevreden.

Ik ben ervan overtuigd dat de afstudeerperiode uitstekende, bruikbare resultaten en ervaringen heeft opgeleverd, voor zowel VI als voor mijzelf.

Dankwoord

Graag wil ik deze scriptie afsluiten met het bedanken van alle mensen die betrokken zijn geweest bij mijn afstudeerproject en de totstandkoming van deze scriptie.

In de eerste plaats is dit Marcel Verbruggen. Als technisch begeleider stond je me terzijde met advies, technisch inzicht en ervaring. Door mij de tijd en ruimte te gunnen zelf te experimenteren en ontdekken, heb ik de kans gehad mijn kennis van netwerken op een hoger niveau te krijgen. Uiteindelijk zelfs hoger dan ik vooraf had gehoopt en gedacht. Als ik echter hulp nodig had stond je altijd klaar om duidelijk (en desnoods twee of drie keer…) uit te leggen hoe iets in elkaar zat en/of een duwtje in de goede richting te geven. Ook was jouw enthousiasme voor het vakgebied netwerken, en alles wat ermee te maken heeft, een motivatie tijdens het project om te blijven proberen en leren. Voor dit alles en meer is mijn dank groot.

Als tweede wil ik Maurice Jansen bedanken die, als mijn stagebegeleider en als groupleader van de afdeling IT Infra./Projects, mijn afstuderen mogelijk heeft gemaakt. Het managementperspectief dat je leverde op de opdracht heeft mijn inzicht in het schrijven van duidelijke documentatie vergroot en mij geleerd vanuit de gehele organisatie te kijken naar een opdracht en oplossing. Je hebt behulpzame en opbouwende feedback geleverd die de kwaliteit van het eindresultaat en vooral de onderbouwing erachter ten goede is gekomen. Als laatste wil ik je apart bedanken voor het mogelijk maken van een bezoek aan het bagagesysteem van Schiphol; een unieke kans die ik samen met de andere stagiaires heb gekregen. Een hele ervaring.

Mijn afstudeerbegeleider vanuit Fontys, Tiemen Wijnja, wil ik bedanken voor geleverde hulp tijdens het schrijven van deze scriptie en het duidelijk maken van het proces dat tijdens het afstuderen moest worden doorlopen.

Ook Arjan Starink en Vincent Kremers wil ik bedanken, voor hun input vanuit de afdelingen Control Support en Service DPP bij het opstellen van de eisen en wensen van VI.

Verder wil ik mijn medestagiaires bedanken: Robin Derksen, Qian Li, Shahriyar Nasrmalek, Twan Verbunt en Stef van Zantvoort. Onze lunch- en koffiepauzes en de humor tussendoor zorgde voor een welkome afwisseling en hebben bijgedragen aan de gezellige sfeer tijdens het afstuderen.

Ook mijn collegae van de afdelingen IT Infra./Projects en IT Infrastructure wil ik bedanken voor de sfeer en gezelligheid.

Verder wil ik ook mijn vader, mijn moeder, mijn zus , mijn “schoonbroer” Roel, mijn collega Stefan Roelofs en mijn voormalige docenten Jacqueline van Erp en Peter van den Broek bedanken voor het lezen en bekritiseren van mijn scriptie. Zonder jullie was dit resultaat er niet in deze vorm geweest!

Iedereen die bij mijn afstuderen, scriptie en studie betrokken is geweest: Hartelijk Bedankt!

Literatuurlijst

BRONNEN

[1] Vanderlande Industries
Bedrijfsprofiel, 2010
http://vanderlande.nl/web/Over-Vanderlande/Bedrijfsprofiel.htm

[2] Vanderlande Industries
Algemene informatie over producten en diensten, 2010
http://vanderlande.nl/web/Distributie.htm
http://vanderlande.nl/web/Bagageafhandeling.htm
http://vanderlande.nl/web/Parcel-Postal-1.htm

[3] Marcel Verbruggen, Vanderlande Industries
VPN Architectural Design Specifications, 16 Nov 2009

[4] FEI Company
RAPID - Remote Diagnostics Program, 2008
Whitepaper

ACHTERGROND CITATEN

[I] **Oude Testament, Ecclesiates 3:1-8**
Een onderdeel van vers 3:1-8 uit het Oude Testament. Er werd lang gedacht dat het boek Ecclesiates is geschreven door Koning Solomon, al wordt er tegenwoordig getwijfeld aan deze opvatting. De gebruikte taal en structuur zijn van een latere periode.

[II] **Albert Szent-Györgyi von Nagyrápolt**
Boedapest, 16 September 1893 - Woods Hole, Massachusetts, 22 Oktober 1986
Hongaars arts en onderzoeker die in 1937 de Nobelprijs voor de Fysiologie of Geneeskunde kreeg voor onder andere zijn werk over vitamine C. Het meeste onderzoek hiervoor verrichte hij tussen 1920 en 1926 aan de Rijksuniversiteit Groningen.

[III] **Marcus Tullius Cicero**
Arpinum, 6 januari 106 v.Chr. - Caieta, 7 december 43 v.Chr.
Romeins staatsman, filosoof en advocaat. Hij wordt beschouwd als één van de beste sprekers ooit en is één van de weinige Romeinen van wie een vrij volledige biografie beschikbaar is.