Scriptie

Sentia B.V.

Vak-code: Afstuderen (TICT-AFSTUD-12)

Klas: SV3A

Versie: 1.0

Datum: 15-3-2016

R. Badal	1607426	ricky.badal@student.hu.nl
Bart Bosma	Eerste examinator	bart.bosma@hu.nl
Jos van Dongen	Tweede examinator	jos.vandongen@hu.nl

Scriptie, Utrecht, 15-3-2016

R. Badal

Versiebeheer

Hieronder volgt het versiebeheer.

Versie	Datum	Opmerkingen
0.1	16-9-2015	Origineel document opgesteld.
0.2	08-02-2015	Feedback docentbegeleider verwerkt.
0.3	11-02-2016	Feedback Jos verwerkt en structuur aangepast.
0.4	17-02-2016	Afspraak gemaakt met Jos en structuur van de scriptie aangepast.
0.5	23-02-2016	Commentaar Jos verwerkt. Advies en aanbeveling aangepast.
0.6	01-03-2016	Finale feedback Jos verwerkt. Lay-out aangepast.
0.7	01-03-2016	Verwijzingen aangepast en bijlagen toegevoegd.
0.8	08-03-2016	Feedback Roland Bijbank verwerkt.
0.9	10-03-2016	Hoofdstuk nummering toegevoegd.
1.0	15-03-2016	Finale versie scriptie.

TABEL 1; VERSIEBEHEER

Goedkeuring

Hieronder volgt het goedkeuringstabel

Naam	Functie	Datum	Handtekening
C. Dobbelaar	C.T.O. Sentia		
J. van Dongen	Docent begeleider HU		
R. Badal	Afstudeerder		

TABEL 2; GOEDKEURINGSTABEL

Voorwoord

De scriptie die voor u ligt is het einddocument dat tot stand gekomen is gedurende mijn afstudeerperiode. De scriptie is geschreven voor het bedrijf Sentia B.V. in opdracht van de Hogeschool Utrecht.

De scriptie is het resultaat van het onderzoek dat ik uitgevoerd heb naar verschillende firewalls. Op basis van dit onderzoek heb ik het bedrijf advies kunnen geven over wat de best mogelijke firewall is in de huidige infrastructuur van het bedrijf.

Graag zou ik deze mogelijkheid willen gebruik om mijn moeder te bedanken. Tijdens mijn studie heeft mijn moeder altijd voor mij klaargestaan en heeft ze haar best gedaan om mij zo goed mogelijk te helpen. Ook ben ik haar dankbaar voor het maken van mijn ontbijt en lunch gedurende mijn schoolperiode. Op deze manier kon ik net wat langer blijven liggen en was ik goed uitgerust voor de lessen die er kwamen.

Ook wil ik mijn zussen willen bedanken voor alle steun die ze mij gegeven hebben tijdens mijn schoolperiode.

De volgende persoon die ik wil bedanken is mijn vriendin. Als het wat minder ging op school maakte ze mij altijd duidelijk dat ik het wel kon halen.

Ook mijn docent-begeleider, Jos van Dongen, zou ik graag willen bedanken voor alle feedback die hij mij gegeven heeft. Zonder zijn hulp en uitleg zou het voor mij niet mogelijk geweest zijn om mijn scriptie succesvol af te ronden.

Ten slotte wil ik Camiel Dobbelaar bedanken voor de feedback die hij mij gegeven heeft gedurende mijn periode bij Sentia.

Ricky Badal

Utrecht, 15 maart 2016

Managementsamenvatting

Sentia is een bedrijf dat zich specialiseert in het outsourcen van bedrijfskritische IT-diensten. Het motto van het bedrijf is dat 99,9% beschikbaarheid niet goed genoeg is. Daarom streeft het bedrijf ernaar om de IT-diensten die het levert zo goed mogelijk beschikbaar te laten zijn. De diensten die het bedrijf levert aan haar klanten dienen natuurlijk beveiligd te worden, zodat het niet mogelijk is voor derde partijen om informatie te achterhalen uit de aangeboden diensten.

Om deze reden heeft het bedrijf de huidige opdracht geformuleerd voor de student. De opdracht bestaat uit het zoeken naar een backend firewall die het meest voldoet aan de eisen en wensen van het bedrijf en het creëren van een beheerontwerp. De doelstelling van de opdracht is om advies te geven over de best mogelijke firewall. Met de 'best' mogelijke firewall wordt de firewall bedoeld die het meest voldoet aan de eisen en wensen van het bedrijf.

Het project is opgedeeld in verschillende fases om zo op een gestructureerde manier aan te kunnen tonen wat er onderzocht is en hoe de student tot het advies gekomen is. Tijdens het project is in iedere fase een deelproduct tot stand gekomen. Een overzicht van de fases en de deelproducten is hieronder weergegeven.

Initiatiefase

Deelproduct	Afstudeervoorstel

Onderzoeksfase

Deelproducten	Plan van Aanpak
	Onderzoeksrapport

Ontwerpfase

Deelproducten	Functioneel Ontwerp
	Technisch Ontwerp

Validatiefase

Tijdens deze fase is er samen met de bedrijfsbegeleider gekeken naar de geadviseerde pakketten en de gecreëerde ontwerpen (functioneel en technisch).

Implementatiefase

Deelproducten	Testplan
	Proof of Concept

Documentatiefase

Product	Scriptie met advies

In de initiatiefase heeft de student een voorstel geschreven hoe hij denkt het project aan te pakken. Dit voorstel is opgestuurd naar de examencommissie van de Hogeschool Utrecht.

Tijdens de onderzoeksfase heeft de student drie pakketten uit de shortlist met elkaar vergeleken: pfSense, VMWare NSX en Contrail. Tijdens deze fase zijn de eisen en wensen van het bedrijf vastgesteld na het bestuderen van verschillende literatuur en een interview met de CTO van het bedrijf.

Tijdens de ontwerpfase heeft de student een functioneel ontwerp gecreëerd en verschillende technische ontwerpen opgesteld voor de betreffende pakketten.

In de validatiefase zijn deze ontwerpen bekeken en goedgekeurd door de bedrijfsbegeleider.

In de implementatiefase heeft de student de testomgeving beschreven en het proof of concept gedocumenteerd. In het testplan staat beschreven hoe de verschillende pakketten getest worden en hoe de pakketten met elkaar vergeleken worden. In het proof of concept-document zijn de testresultaten van de pakketten gedocumenteerd.

Tijdens de documentatiefase zijn de bevindingen van de student beschreven in de vorm van een scriptie. Aan het eind van de scriptie is er een advies opgesteld welke firewall het meest voldoet aan de eisen en wensen van het bedrijf.

Aan het eind van de implementatiefase is de student tot de conclusie gekomen dat het pakket VMWare NSX het meeste voldoet aan de eisen en wensen van het bedrijf. Tijdens het testen van de pakketten is gebleken dat VMware NSX het beste reageert op de testomstandigheden.

Omdat VMware NSX direct in de huidige omgeving integreert, heeft de firewall kennis van alle virtuele machines. Het voordeel hiervan is dat er beveiligingen geplaatst kunnen worden per virtuele machine. Normaal worden beveiligingen op netwerkniveau gedaan. Twee machines in hetzelfde netwerk hebben dan dezelfde beveiligingen. Met VMWare NSX is het mogelijk om twee machines in hetzelfde netwerk aparte beveiligingen te geven. Ook al zitten de twee machines in hetzelfde netwerk, dan kunnen de beveiligingen alsnog per virtuele machine worden ingesteld.

De kosten van VMware NSX worden per punt geregeld. Per beheerde machine kost VMware NSX 20 punten. Eén punt staat ongeveer gelijk aan € 0,80. Worden er dus bijvoorbeeld drie machines beheerd door VMware NSX, dan zijn dit 60 punten, wat ongeveer gelijk staat aan €48,-.

Om deze redenen geeft de student het bedrijf Sentia het advies om VMware NSX te implementeren.

Inhoudsopgave

1 Inleiding

Dit document is geschreven als verantwoording van de afstudeeropdracht van de student. De student voert de afstudeeropdracht uit bij het bedrijf Sentia. Sentia heeft voor de afstuderende student een afstudeeropdracht geformuleerd. De opdracht bestaat uit onderzoek doen naar een software-gebaseerde backend firewall en het geven van advies dat past bij de eisen en wensen die het bedrijf heeft over de firewall en het beheerontwerp.

Dit document is de verantwoording van het onderzoek en is tot stand gekomen uit eerdere geschreven documenten die deel uitmaken van de afstudeeropdracht van de student. De documenten waardoor de scriptie tot stand is gekomen zijn:

- Afstudeervoorstel
- Plan van Aanpak
- Onderzoeksrapport
- Functioneel Ontwerp
- Technisch Ontwerp
- Testplan
- Proof of Concept

De afstudeeropdracht is tot stand gekomen doordat het bedrijf op gestructureerde wijze wil onderzoeken wat de best mogelijke firewall is voor het bedrijf. Met ‘best mogelijke’ wordt bedoeld dat de firewall moet voldoen aan de eisen en wensen die het bedrijf stelt. Het pakket dat het hoogste scoort in de vergelijkingstabel (zie *shortlist*, pagina 28) kan het best mogelijke pakket zijn. In een productie-omgeving kan de theorie echter verschillen van de praktijk. Om een zo goed mogelijk advies te geven zal er daarom dan ook een Proof of Concept aan het bedrijf worden getoond van de pakketten die er in de shortlist staan. Aan het einde van het onderzoek zal er een conclusie worden getrokken over welk(e) pakket(ten) het beste zijn. In dit document zal duidelijk gemaakt worden hoe de student dit onderzoek heeft aangepakt en wat voor advies er gegeven wordt aan het bedrijf. Ook zullen de stappen worden beschreven die de student heeft genomen om de opdracht zo goed mogelijk uit te voeren.

1.1 Leeswijzer

In deze paragraaf zal de leeswijzer van de scriptie worden beschreven. Het hoofdstuk *De organisatie* beschrijft de indeling van het bedrijf en de taken van de student. In het hoofdstuk *De opdracht* wordt de opdracht van de student beschreven. Het hoofdstuk *Faseringen* beschrijft de faseringen en de hoofd- en deelvragen. In het hoofdstuk *Doelstellingen* worden het type opdracht en de op te leveren producten besproken. Het hoofdstuk *Resultaten* bespreekt de deelproducten die per fase zijn opgeleverd, de eisen en wensen van het bedrijf en de shortlist, samen met de kosten van de implementatie en de beantwoording van de deelvragen. In het hoofdstuk *Conclusie* wordt het advies uitgebracht en de aanbevelingen van de student weergegeven. In het hoofdstuk *Procesevaluatie* wordt een evaluatie van de procesgang beschreven. Na dit hoofdstuk volgen in de Bibliografie de bronnen die gebruikt zijn voor het onderzoek. Ten slotte worden in het hoofdstuk *Bijlagen* de bijlagen weergegeven. Deze bijlagen bestaan uit de volgende documenten: Plan van Aanpak, Afstudeervoorstel, Onderzoeksrapport, Functioneel Ontwerp, Technisch Ontwerp, Testplan en Proof of Concept.

2 De organisatie

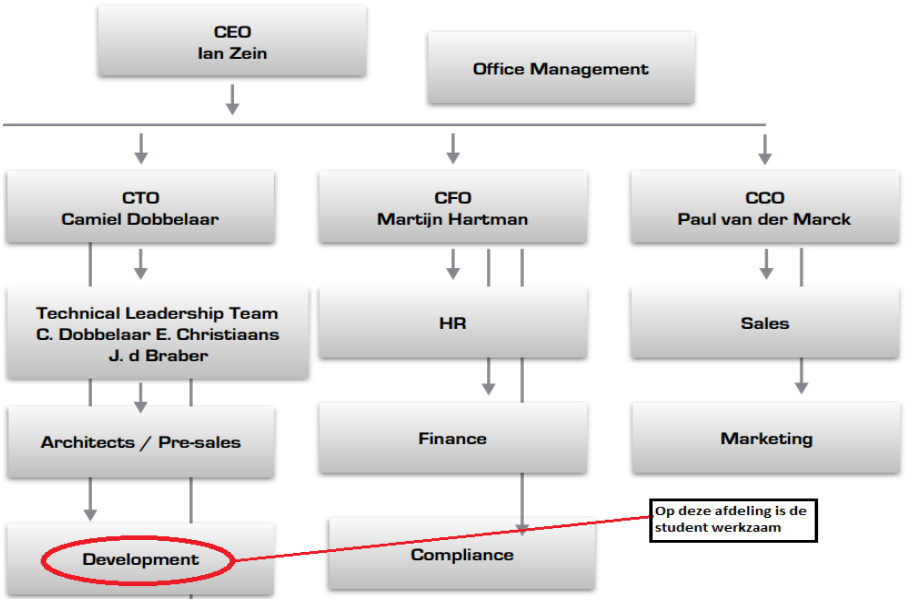
In dit hoofdstuk wordt een korte beschrijving gegeven van het bedrijf waar de student zijn opdracht uitvoert.

2.1 Sentia B.V.

Sentia B.V. is een bedrijf dat zich specialiseert in IT-outsourcing, private en public Cloudoplossingen en Technisch Applicatie Beheer. Sentia B.V. heeft een eigen private Cloudplatform, genaamd Sentia Cloud. Dit Cloudplatform is speciaal ontworpen voor bedrijfskritische applicaties en vanuit dit platform worden er diensten aangeboden aan de klanten. Een aantal klanten van Sentia B.V. zijn Allianz, Achmea, Unigarant, Albelli, Triodos Bank, Ennia Caribe, Amber Alert, ARAG, Univé Verzekeringen en de Consumentenbond.

Sentia B.V. telt ongeveer 70 medewerkers, maar is momenteel hard aan het groeien. Binnen het bedrijf wordt niet gebruikgemaakt van een 'vast' operating system voor de desktop PC's. In principe zijn de medewerkers vrij om te kiezen welk operating system ze draaien. De meest voorkomende operating systems die binnen het bedrijf gebruikt worden zijn Windows, OSx en Linux. Aan de serverkant wordt er voornamelijk gebruikgemaakt van OpenBSD-systemen en Windows 2012R2.

De student is geplaatst op de afdeling Development. Hier werkt de student aan de verbetering en vernieuwing van het Sentiaplatform dat betrekking heeft op de afstudeeropdracht. Zie afbeelding 1.



AFBEELDING 1; ORGANOGRAM SENTIA

2.2 Taken, verantwoordelijkheden en bevoegdheden van de student

De voornaamste verantwoordelijkheden van de student zijn om onderzoek te doen naar een softwaregebaseerde firewall die dient als backend firewall voor de services die Sentia B.V. levert aan haar klanten. Ook het opzetten van een beheerontwerp, zodat het bedrijf de nieuwe firewall kan beheren, is een verantwoordelijkheid van de student. Er zal dus een ontwerp worden gemaakt van hoe men de nieuwe firewall kan beheren. De student heeft de bevoegdheid om gebruik te maken van apparatuur van het bedrijf om zo testopstellingen te kunnen maken. Door gebruik te maken van de testopstelling kan de student onderzoek doen naar de verschillende onderwerpen en pakketten. Dit onderzoek wordt gebruik ter ondersteuning van het uiteindelijke advies dat aan het bedrijf zal worden gegeven. De bevindingen zijn gedocumenteerd in het onderzoeksrapport, zie *'Bijlagen – Onderzoeksrapport'*, op pagina 94.

3 De opdracht

De opdracht van de student bestaat uit onderzoek doen naar een softwaregebaseerde backend firewall en het geven van advies over welke firewall het beste voldoet aan de eisen en wensen die het bedrijf heeft voor de firewall en het beheerontwerp. Het beheerontwerp heeft als doel dat het bedrijf het beheer na de stage van de student kan overnemen. Het uiteindelijke advies gaan over welk pakket uit de shortlist het beste voldoet aan de eisen en wensen. Het onderzoek dient dus als verantwoording voor de pakketkeuze. De opdracht is concreet te formuleren als:

Doe onderzoek naar een softwaregebaseerde backend firewall en geef advies over de beste firewall die voldoet aan de eisen en wensen die het bedrijf heeft over de firewall en het beheerontwerp.

3.1 Aanleiding

Sentia B.V. maakt momenteel gebruik van fysieke firewalls met het besturingssysteem OpenBSD. Deze fysieke firewalls dienen als 'front-end' firewalls voor de huidige infrastructuur. Omdat de infrastructuur in de afgelopen jaren flink gegroeid is, heeft het bedrijf als wens om een extra laag beveiliging toe te passen (de 'backend' firewall) voor de groeiende infrastructuur. De aanleiding voor deze opdracht is dat het bedrijf een vergelijking wenst van verschillende firewalls en functies om te zien welke firewalls aan de eisen en wensen van het bedrijf voldoen. Daarna wil het bedrijf een advies krijgen over de pakketkeuze om zo de best mogelijke firewall te vinden die het meeste voldoet aan de eisen en wensen van het bedrijf.

3.2 Wijziging Plan van Aanpak

In het Plan van Aanpak van de student stond een probleemstelling beschreven. Deze probleemstelling is veranderd gedurende de periode dat de student werkzaam is bij het bedrijf. De huidige vraagstelling kan beschreven worden als een kans voor het bedrijf waarin onderzocht wordt welke firewall het beste in de huidige infrastructuur past en het beste voldoet aan de eisen en wensen die het bedrijf stelt. Met deze kans kan er een advies worden gegeven over de best mogelijk firewall voor het bedrijf en krijgt het bedrijf een beter inzicht in welke aspecten van de huidige situatie niet voldoen aan de gewenste eisen en wensen.

3.3 De vraagstelling

In de huidige situatie wordt Linux gebruikt als virtuele firewall. Deze firewall maakt het mogelijk om netwerken te beveiligen en maakt gebruik van de Linux firewall kernel module om pakketten te filteren. Om de verschillende netwerken te beveiligen wordt gebruikgemaakt van het programma 'IPTables'. IPTables is een command-lineprogramma voor Linux dat de regels toepast in de firewall kernel module. Om firewall rules te beheren dienen er via de command-line commando's uitgevoerd te worden en dient de beheerder kennis te hebben van het programma IPTables om de structuur van de verschillende rules te begrijpen. Het bedrijf heeft de wens om een vergelijking te maken van verschillende firewalls en functies om te zien welke firewalls aan de eisen en wensen van het bedrijf voldoen en in de huidige infrastructuur passen. Voor een overzicht van de eisen en wensen, zie paragraaf 'Eisen en wensen' op pagina 25.

Bij het onderzoeken van de backend firewall moet er rekening gehouden worden met een aantal factoren, namelijk:

- Kosten (voorkeur heeft Open Source, een betaald alternatief mag ook, mits dit binnen het bedrijf past qua infrastructuur en eisen en wensen)
- Performance (de firewall moet onder hoge verkeersdrukte optimaal kunnen presteren)
- Redundantie/high availability (mocht de firewall uitvallen, dan dient er een back-up firewall geactiveerd te worden en de taken over te nemen)
- Integratie met VMWare (de firewall dient implementeerbaar te zijn in de huidige omgeving)
- Routeringsprotocollen (ospf, etc.)
- Andere protocollen (802.1q, vxlan)
- Beheerbaarheid (de firewall dient vanuit een centrale plek beheerbaar te zijn)
- Ontwikkelingsuren (om het bruikbaar te krijgen; dit mag niet te veel tijd kosten)

Omdat de huidige front-end firewalls op het open-source systeem OpenBSD draaien en het bedrijf zo flexibel mogelijk wil blijven, heeft een open-source firewall de voorkeur.

Een test met een commercieel alternatief is wenselijk om de vergelijking tussen een commerciële en een gratis variant te vergelijken.

3.4 Hoofdvraag

De hoofdvraag is als volgt geformuleerd: *"Welk type firewall voldoet het meest aan de gestelde eisen van het bedrijf en is het meest geschikt voor de huidige infrastructuur?"*

3.5 Deelvragen

Om de hoofdvraag goed te kunnen beantwoorden, is een aantal deelvragen geformuleerd.

- Welke verschillen zijn er tussen een open source (gratis) firewall en een closed source (betaalde) firewall?
- Welke firewallfuncties dienen beschikbaar te zijn om aan de eisen van het bedrijf te voldoen? (To Be)
- Welke risico's zijn er bij het implementeren van een firewall in een bestaande omgeving?
- Op welke manier wordt de firewall gemonitord?
- Wat zijn de voor- en nadelen van een virtuele firewall ten opzichte van een fysieke firewall?

3.6 Onderzoeksmethoden

Om zo goed mogelijk antwoord te kunnen geven op de hoofdvraag en deelvragen zullen er verschillende onderzoeksmethoden gebruikt worden. Hieronder, in tabel 3, staat een overzicht van de methoden die gebruikt worden tijdens de afstudeeropdracht.

TABEL 3; ONDERZOEKSMETHODEN

Vragen	Methoden	Opmerkingen
Welke verschillen zijn er tussen een open source (gratis) firewall en een closed source (betaalde) firewall?	Research	Door middel van deze methode kan de student erachter komen welke functies beschikbaar zijn bij een betaalde firewall en of dezelfde functies ook beschikbaar zijn bij een open source alternatief.
Welke firewallfuncties dienen beschikbaar te zijn om aan de eisen van het bedrijf te voldoen?	Interview/ MoSCoW analyse	Door interviews te houden kan de student deze deelvraag beantwoorden. Deze functies kunnen omgezet worden in eisen en wensen in de MoSCoW-analyse.
Welke risico's zijn er bij het implementeren van een firewall in een bestaande omgeving?	Research	Tijdens de onderzoeksfase zal er een testomgeving worden opgezet. In deze omgeving kan de student achter de risico's komen van het implementeren van een firewall in een bestaande omgeving.
Op welke manier wordt de firewall gemonitord?	Interview	Door middel van interviews kan de student erachter komen hoe bepaalde services gemonitord worden binnen het bedrijf. Ook kan de student voorstellen om de firewall mee te nemen in de huidige monitoring.
Wat zijn de voor- en nadelen van een virtuele firewall ten opzichte van een fysieke firewall?	Research/testen in een testomgeving	Door middel van het testen van bepaalde opstellingen kan de student erachter komen wat de voor- en nadelen zijn van een virtuele en een fysieke firewall.

4 Faseringen

Om de opdracht zo gestructureerd mogelijk aan te pakken, wordt er een aantal fases doorlopen, namelijk;

- Initiatiefase
- Onderzoeksfase
- Ontwerpfase
- Validatie (besluitvorming over het advies)
- Implementatiefase
- Documentatiefase

4.1 Initiatiefase

Tijdens deze fase wordt er gekeken hoe het project aangepakt kan worden en wordt er door de student een voorstel geschreven voor de afstudeeropdracht. Dit voorstel is een voorlopig voorstel van de aanpak en beschrijving van het project.

4.2 Onderzoeksfase

Tijdens deze fase wordt er een Plan van Aanpak schreven. In dit Plan van Aanpak beschrijft de student de opdracht en de manier waarop de student denkt het project aan te pakken. Ook zal er onderzoek gedaan worden naar verschillende firewalls/pakketten. De verschillende pakketten zullen met elkaar vergeleken worden en aan het eind van deze fase zal er een keuze worden gemaakt voor het beste pakket/pakketten. Het doel van deze fase is om onderzoek te doen naar welk pakket het beste voldoet aan alle eisen en wensen van het bedrijf en het geven van advies met betrekking tot deze eisen en wensen.

4.3 Ontwerpfase

Tijdens deze fase zal er een ontwerp worden gemaakt met het gekozen pakket(ten). Er zal worden gekeken waar de firewall het best geplaatst kan worden in de huidige infrastructuur. Dit zal in overeenstemming met de begeleidende bedrijfsleider worden gedaan. Het doel van deze fase is om een ontwerp te maken van de infrastructuur met de implementatie van de nieuwe backend firewall. Ook zal er een ontwerp worden gemaakt voor het beheer. Het doel van dit beheerontwerp is om het beheer over te dragen aan het bedrijf nadat de student klaar is met zijn stage.

4.4 Validatiefase

Tijdens deze fase zal er gekeken worden naar het functionele en technische ontwerp van het geadviseerde pakket(ten) en het beheerontwerp. Er zal samen met de bedrijfsbegeleider worden gekeken of het pakket en de ontwerpen voldoen aan de eisen die het bedrijf stelt aan de nieuwe backend firewall en het beheerontwerp. Indien het bedrijf akkoord gaat met de gemaakte keuzes, kan er door worden gegaan naar de volgende fase, de implementatiefase. Indien het bedrijf niet akkoord is met de gemaakte keuzes, dan zal er terug worden gegaan naar de onderzoeksfase. Het doel van de validatiefase is dus om samen met het bedrijf te kijken of de wensen, eisen en gemaakte keuzes goed verwerkt zijn en, indien akkoord, door te gaan naar de implementatiefase.

4.5 Implementatiefase

In deze fase zal het 'proof of concept' worden gebouwd. Dit houdt in dat de student een testopstelling zal maken met het gekozen pakket en ontwerp en dit zal tonen aan de bedrijfsbegeleider. Tijdens het proof of concept moet de student kunnen aantonen dat alle wensen en eisen van het bedrijf zijn meegenomen. De student dient het concept werkende te tonen aan de bedrijfsbegeleider. Dit kan gedaan worden door middel van een testplan. In het testplan staan alle functies die moeten werken en moeten voldoen aan de wensen van de klant. Het doel van deze fase is dus om het proof of concept werkend te laten zien met inachtneming van de eisen die Sentia B.V. stelt aan het gekozen pakket.

4.6 Documentatiefase

Tijdens deze fase zullen de bevindingen worden gedocumenteerd. De bevindingen per fase zullen apart worden gedocumenteerd in aparte documenten (bijlagen). De bevindingen die opgedaan en gedocumenteerd zijn in de onderzoeksfase kunnen als handleiding gebruikt worden voor het installeren en configureren van eventuele software. Het beheer van het pakket in de ontwerpfase zal ook worden gedocumenteerd in de vorm van een beheerplan. Het doel van deze fase is om op een gestructureerde wijze aan te tonen hoe de student de functionele eisen en wensen heeft onderzocht en het onderzoek heeft aangepakt. Aan het eind van het onderzoek zal er een advies worden geschreven.

5 Doelstelling

De doelstelling van de afstudeeropdracht is om een advies te geven met betrekking tot de backend firewall en de beveiligingsfuncties hiervan, en aan te geven welke firewall het best past in de huidige infrastructuur van het bedrijf. Ook dient er advies gegeven te worden over het beheren van de firewall en dient deze gedocumenteerd te worden in een beheerplan. De resultaten van het onderzoek naar het product zullen gedocumenteerd worden en er zal een proof of concept worden gebouwd om de functies van de firewall werkend aan het bedrijf te laten zien. Dit zal worden aangetoond aan het einde van de afstudeerstage, in maart-april 2016.

5.1 Type opdracht

De opdracht die de student zal moeten uitvoeren is een ontwerp-, advies- en onderzoeksopdracht. Er zal onderzoek gedaan worden naar het product (de backend firewall) en een ontwerp gemaakt worden voor het beheer. In dit ontwerp zal duidelijk worden gemaakt hoe het bedrijf de nieuwe firewall kan beheren. Ook zal er aan het einde van de scriptie een advies worden gegeven over de pakketkeuze.

5.2 Op te leveren producten

Het project is opgedeeld in verschillende fases. Per fase worden er (deel)producten opgeleverd. In deze paragraaf wordt beschreven welke (deel)producten er per fase worden opgeleverd.

- Initiatiefase
  - Afstudeervoorstel
- Onderzoeksfase
  - Plan van Aanpak
  - Onderzoeksrapport
- Ontwerpfase
  - Functioneel Ontwerp
  - Technisch Ontwerp
- Validatiefase
  Tijdens deze fase wordt er met de bedrijfsbegeleider gekeken naar de opgeleverde (deel)producten en ontwerpen. Indien het bedrijf hiermee akkoord gaat, dan kan er doorgegaan worden naar de volgende fase, de implementatiefase. Indien de (deel)producten en/of ontwerpen niet akkoord zijn, gaat de student terug naar de ontwerpfase om de gewenste wijzigingen aan te brengen in de (deel)producten en ontwerpen.
- Implementatiefase
  - Testplan
  - Proof of Concept
- Documentatiefase
  - Scriptie met advies

5.3 Kwaliteitsborging

Om de kwaliteit van de op te leveren producten zo hoog mogelijk te houden zijn er afspraken gemaakt met het bedrijf. De afspraken zijn als volgt.

- De voortgang zal wekelijks besproken worden met de opdrachtgever.
- Feedback voor de op te leveren producten zal binnen een week worden verwerkt door de student.
- De op te leveren documenten zullen nagekeken worden op taal- en spelfouten.
- De technische documentatie zal door technici worden nagekeken.
- Er zullen interviews plaatsvinden om onduidelijkheden te voorkomen.

6 Resultaten

In dit hoofdstuk zullen de resultaten worden beschreven die per fase zijn behaald. Ook de beantwoording van de deelvragen wordt gedocumenteerd worden in dit hoofdstuk.

6.1 Initiatiefase

Tijdens deze fase wordt bekeken hoe de student het project het beste kan aanpakken. Er wordt een afstudeervoorstel geschreven voor de examencommissie waarin staat beschreven hoe de student het project wil aanpakken, samen met een planning. De bevindingen van deze fase zijn terug te vinden in het hoofdstuk *'Bijlagen – Afstudeervoorstel'* op pagina 75.

6.2 Onderzoeksfase

In deze fase heeft de student een literatuurstudie uitgevoerd naar verschillende firewalls, zie sub-paragraaf Theoretisch Kader op pagina 21. Ook zijn de eisen en wensen van het bedrijf achterhaald door middel van een interview, zie sub-paragraaf Eisen en Wensen op pagina 25. De bevindingen van deze fase zijn gedocumenteerd in het onderzoeksrapport, zie het hoofdstuk *'Bijlagen – Onderzoeksrapport'*. De volgende onderwerpen zullen in deze fase worden beschreven.

- Huidige situatie
- Gewenste situatie
- Theoretisch kader
- Eisen en wensen
- Shortlist
- Kosten
- Beantwoording deelvragen

6.2.1 Huidige situatie

In deze paragraaf zal de huidige situatie van het bedrijf worden beschreven.

In de huidige situatie wordt het operating system Linux gebruikt als virtuele firewall. Deze firewall maakt het mogelijk om netwerken te beveiligen en maakt gebruik van de Linux firewall kernel module om pakketten te filteren. Om de verschillende netwerken te beveiligen wordt er gebruikgemaakt van het programma 'IPTables'. IPTables is een command-line programma voor Linux die de regels toepast in de firewall kernel module. Om firewall rules te beheren dienen er via de command-line commando's uitgevoerd te worden en dient de beheerder kennis te hebben van het programma IPTables om de structuur van de verschillende rules te begrijpen.

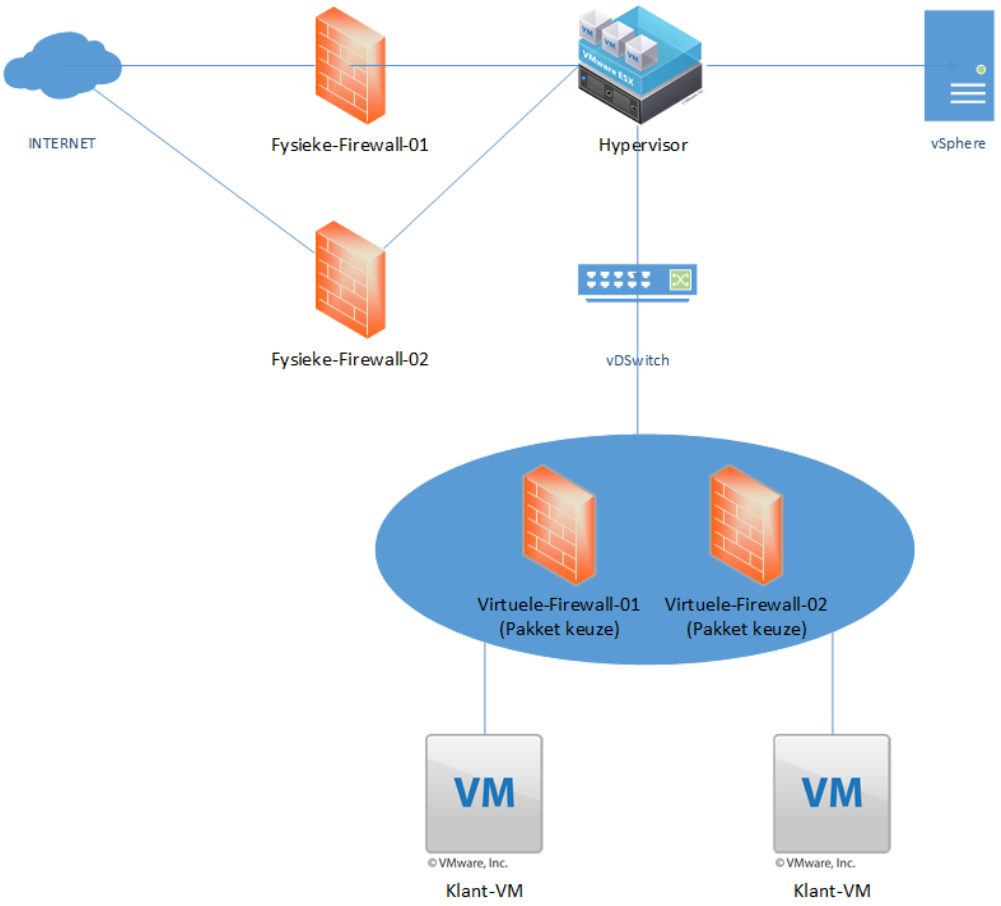
Het bedrijf heeft de wens om een onderzoek uit te laten voeren en een advies te laten uitbrengen over de verschillende firewalls en functies die aan de eisen en wensen van het bedrijf voldoen en in de huidige infrastructuur passen. Voor een overzicht van de eisen en wensen, zie de paragraaf 'Eisen en wensen' op pagina 25. Aan het eind van het onderzoek zal er een conclusie getrokken worden waarin duidelijk wordt gemaakt welke pakketten er het beste

passen in de huidige infrastructuur en het meeste voldoen aan de eisen en wensen van het bedrijf.

6.2.2 Gewenste situatie

In de gewenste situatie zal de huidige firewall vervangen worden door een ander pakket. Het bedrijf heeft een aantal eisen en wensen waardoor het beheer en de functionaliteit van de firewall beter te overzien zijn. De firewall dient bijvoorbeeld beheerbaar te zijn door medewerkers weinig verstand hebben van de firewall.

Een overzicht van de gewenste situatie vindt men in afbeelding 2. De virtuele firewall zal nog steeds dubbel worden uitgevoerd (om de beschikbaarheid te verhogen) en de firewall zal voor dezelfde taken zorgen als in de huidige situatie. De nieuwe virtuele firewall zal echter aan de nieuwe eisen en wensen van het bedrijf moeten voldoen.



AFBEELDING 2; GEWENSTE SITUATIE

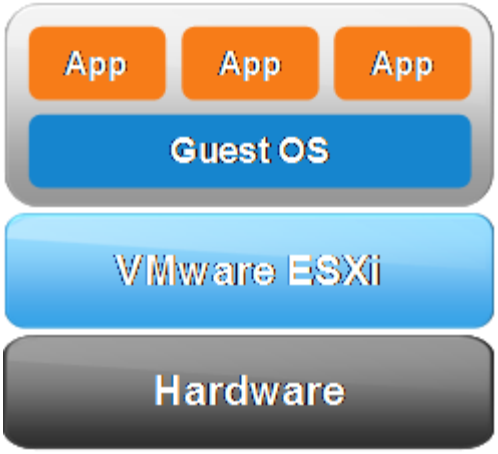
6.2.3 Theoretisch kader

Deze paragraaf is bedoeld ter ondersteuning van het vaststellen van de eisen voor het eindpakket. Er zullen verschillende technische begrippen worden uitgelegd en er zal duidelijk worden gemaakt welke firewallfuncties waarvoor dienen. Dit hoofdstuk vormt de wetenschappelijke basis van het onderzoek dat de student uitvoert gedurende zijn afstudeerperiode bij het bedrijf.

Hypervisor

Een hypervisor is een fysieke machine/server waarop een licht besturingssysteem wordt geïnstalleerd. Een hypervisor maakt het mogelijk om op een fysieke machine virtuele machines te creëren en te beheren. Hierdoor kunnen meerdere machines/besturingssystemen op dezelfde fysieke machine draaien.

Als hypervisor wordt er binnen het bedrijf gebruikgemaakt van VMWare ESXi versie 5.5. VMWare ESXi is een licht besturingssysteem dat maar 3-400 MB groot is. Het gebruikt dus niet veel resources van de fysieke machines; hierdoor blijven de resources beschikbaar voor de virtuele machines. In afbeelding 3 is afgebeeld hoe een hypervisor werkt.



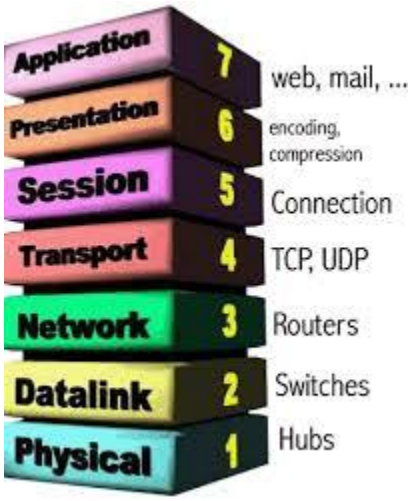
AFBEELDING 3; HYPERVISOR (VMWARE, VIRTUALIZATION, 2009)

Afbeelding 3 laat zien dat VMWare ESXi op de hardware draait. In VMWare ESXi kunnen verschillende virtuele machines worden aangemaakt met elk hun eigen besturingssysteem (Guest OS). Op deze virtuele machines kunnen verschillende applicaties draaien, bijvoorbeeld een web-, ftp- of fileserver. (Revelle, 2011) (VMWare, Virtualization, 2009).

Netwerkvirtualisatie

Netwerkvirtualisatie houdt in dat er logische, virtuele netwerken gecreëerd kunnen worden die onafhankelijk van elkaar op elk type hardware kunnen draaien. Met netwerkvirtualisatie kunnen fysieke netwerken gevirtualiseerd worden. Hierdoor hoeft er geen aparte hardware te worden gekocht voor een router of switch en hoeven er geen fysieke computers aangeschaft te worden om als server te dienen voor het bedrijf.

De verschillende services die normaal fysiek worden aangeboden, zoals storage, firewall of fysieke switches en/of routers, kunnen dus allemaal gevirtualiseerd worden. Er is in theorie maar één fysiek apparaat nodig, de hypervisor, om alle (netwerk)componenten te kunnen virtualiseren. Door middel van netwerkvirtualisatie kunnen alle 7 lagen van het OSI-model gevirtualiseerd worden. Dit houdt in dat applicaties zoals web en mailserver ook virtueel gecreëerd kunnen worden en onderdeel zijn van het virtuele netwerk (Onisick, 2013) (SDXcentral, 2015). Een voorbeeld van het OSI-model is te zien in afbeelding 4.



AFBEELDING 4; OSI-MODEL (IDEMDITO, 2005)

Firewall

Een firewall is applicatie die het mogelijk maakt om een netwerk of netwerken te controleren op het verkeer dat binnenkomt en naar buiten gaat. Er kunnen verschillende services of protocollen geblokkeerd worden tussen netwerken. Een firewall kan op verschillende manieren in een netwerk worden geplaatst. Zo kan er op een firewall bijvoorbeeld worden ingesteld dat netwerk A netwerk B niet mag bereiken, maar netwerk B mag netwerk A wel bereiken (WebOPedia, 2015). Er zijn veel verschillende typen firewalls. Een overzicht van de verschillende type firewalls staat hieronder.

Packet filtering firewall

Een packet filtering firewall kijkt op laag 4 van het OSI-model (de TCP/UDP laag). Door beveiligingen toe te passen wordt er gekeken of een IP-pakket wordt toegelaten of afgewezen. Ook kijkt dit type firewall naar de destination port en het source IP-adres. Een packet filtering firewall kan bijvoorbeeld al het verkeer naar de SSH port (22) verbieden. Het protocol zelf (SSH) kan niet worden geblokkeerd. Als SSH dus op een andere port draait, kan er nog steeds een connectie worden opgezet (TechTarget, 2015).

Application layer firewall

Een applicatie layer firewall functioneert op applicatieniveau (laag 7 van het OSI-model). Er wordt in eerste instantie ook op de TCP/UDP-laag gekeken, vervolgens wordt bepaald of een stukje software of de pakketten worden doorgelaten of tegen worden gehouden.

Bij een applicatie layer firewall wordt er op protocolniveau gekeken. Zo kan bijvoorbeeld SSH op een andere poort alsnog worden geblokkeerd (Greene, 2014).

Stateless firewall
Dit is een firewall die elk pakketje dat het netwerk binnenkomt individueel behandelt. Er wordt geen informatie opgeslagen over bijvoorbeeld een SYN-pakket (request) en een ACK-pakket (akkoord). Dit betekent dus dat er geen connectie wordt gelegd als er nog een ACK moet worden teruggestuurd. Dit type firewall wordt niet vaak in het bedrijfsleven gebruikt (Elsherbeny, 2014).

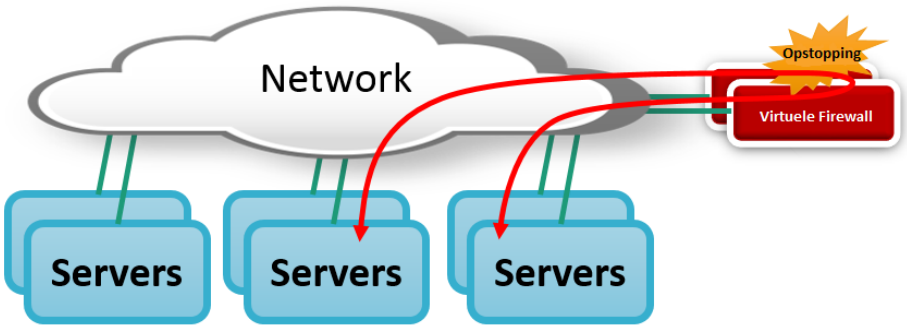
Stateful firewall
In tegenstelling tot de stateless firewall, houdt de stateful firewall wel informatie bij. Als er bijvoorbeeld een SYN-pakket (request) komt, wordt bekeken of er voor diezelfde sessie ook een ACK-pakket (akkoord) uitgaat. Zo kan de firewall sessie-informatie bijhouden.

De variant stateful firewall is toegepast in de huidige infrastructuur van het bedrijf, omdat deze variant de optie heeft om sessie-informatie van verkeer bij te houden. Het dataverkeer tussen zender en ontvanger wordt inhoudelijk geanalyseerd en er wordt verder gekeken dan alleen het IP-adres en het poortnummer. De inhoud van de pakketjes worden bekeken en op basis van de inhoud kunnen de pakketjes verschillend behandeld worden: toegestaan, geweigerd, of met een andere prioriteit doorgestuurd (informIT, 2005).

Distributed firewall
Bij een gedistribueerde firewall zit de firewall geïmplementeerd in de hypervisor. Hierdoor is er geen aparte virtuele machine nodig die de rol van firewall vervult. Alle machines die op de hypervisor zijn aangemaakt, zijn bekend bij een gedistribueerde firewall. Dit maakt het mogelijk om voor elke virtuele machine een eigen aparte firewall te creëren. Zo kan elke klant dus haar eigen firewall hebben.

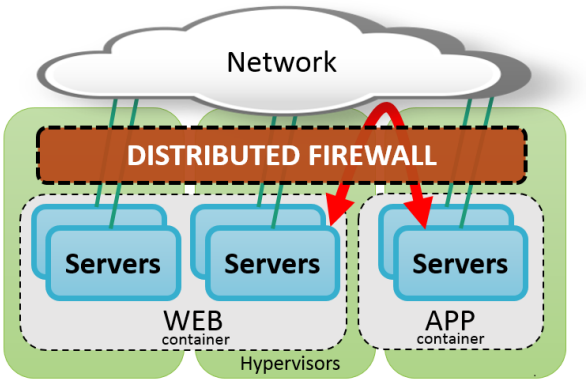
Bij een virtuele stateful firewall wordt er een virtuele machine aangemaakt en worden de machines die beschermd moeten worden aangesloten op de virtuele firewall. Als een machine dus niet aangesloten zit op de firewall, dan heeft deze machine geen bescherming.

In afbeelding 5 is een voorbeeld van een virtuele stateful firewall afgebeld en het gevaar waardoor dat het netwerk hiermee kan lopen.



AFBEELDING 5; STATEFUL FIREWALL GEVAAR (VMWARE, FIREWALL, 2013)

In afbeelding 6 is een voorbeeld van een gedistribueerde firewall getoond. In deze omgeving maakt de firewall deel uit van de hypervisor. Er hoeft dus geen aparte virtuele machine aangemaakt te worden om als firewall te functioneren. Dit heeft als voordeel dat de gedistribueerde firewall meer resources tot zijn beschikking heeft en kennis heeft van elke virtuele machine die geïnstalleerd is op de hypervisor. Op deze manier kan er voor elke virtuele machine een aparte virtuele firewall worden gecreëerd (FAQs, 2013) (TechTarget, 2014).



AFBEELDING 6; DISTRIBUTED FIREWALL (VMWARE, FIREWALL, 2013)

Software Defined Networking

Software Defined Networking (SDN) is een architectuur die het mogelijk maakt om dynamisch met netwerken om te gaan. Door middel van SDN kan een netwerk 'geprogrammeerd' worden en kunnen er templates gemaakt worden van standaard netwerken. Zo kan er bijvoorbeeld een template worden gemaakt van een netwerk dat bestaat uit de volgende onderdelen:

- Router
- Switch
- DHCP-server
- Webserver

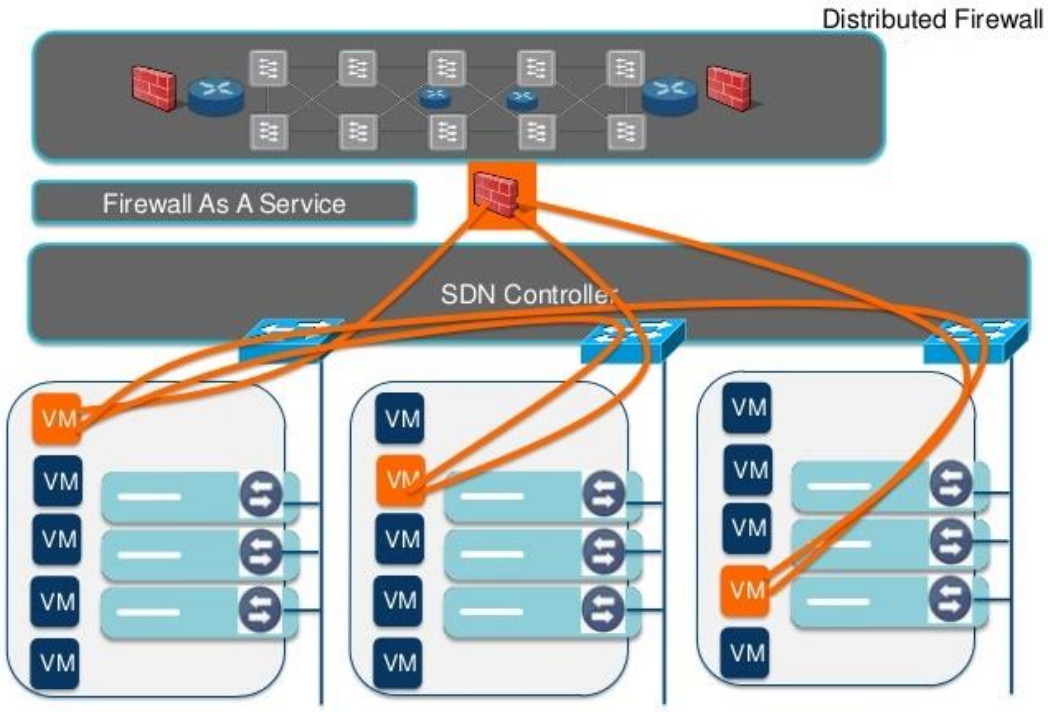
Omdat dit type netwerk gebruikt kan worden voor verschillende klanten, kan hier een template van worden gemaakt en kan dit voor elke klant automatisch worden uitgerold. SDN maakt het mogelijk om verschillende netwerken op een centrale plek te beheren door middel van een SDN controller. Op deze controller zijn alle netwerken zichtbaar en kunnen er firewall rules worden aangemaakt voor de verschillende netwerken. De architectuur die SDN gebruikt voldoet aan de volgende functies:

- Direct programmeerbaar: Netwerken kunnen geprogrammeerd worden en kunnen automatisch worden uitgerold.
- Dynamisch: De verschillende netwerken kunnen dynamisch worden aangepast. Zo kan het netwerk worden aangepast aan de wensen van de klant.
- Centraal beheer: Omdat er in Cloud computing veel servers en services worden aangeboden maakt SDN het mogelijk om alle servers en services centraal te beheren. Zo heeft een netwerkbeheerder direct overzicht over het gehele netwerk.
- Programmeerbare configuraties: De functies die een netwerk kan bieden zijn door middel van SDN ook programmeerbaar. Zo kan het netwerk of een server automatisch

beveiligd worden door middel van standaard firewallregels die automatisch geïntegreerd kunnen worden in een netwerk.

- Open standaarden: Door gebruik te maken van open standaarden kan de SDN-controller geïmplementeerd worden in verschillende omgevingen en is de controller niet afhankelijk van de vendor (fabrikant).

De functies die hierboven staan beschreven komen terug in de eisen en wensen die het bedrijf heeft voor het nieuwe pakket. Afbeelding 7 toont een voorbeeld van een gedistribueerde firewall met een SDN controller (OpenNetworking, 2015) (NetworkComputing, 2012).



AFBEELDING 7; SDN-CONTROLLER (BANNAI, 2013)

6.2.4 Eisen en wensen

In deze paragraaf zullen de eisen en wensen in kaart worden gebracht die het bedrijf stelt aan het eindpakket. De eisen en wensen zijn tot stand gekomen na de literatuurstudie en het interviewen van de CTO van het bedrijf. In tabel 4 staat een overzicht van de eisen en wensen waaraan het pakket zal moeten voldoen.

TABEL 4; EISEN EN WENSEN (MOSCOW ANALYSE)

Eis/Wens	Must have	Should have	Could have	Won't have
Performance/Multi-CPU	X			
High Availability	X			
Beheerbaarheid (Centraal)	X			
Automatisering	X			
Monitoring	X			
IPv6 routering		X		
VXLAN		X		
Open source		X		
Distributed firewall		X		
QoS			X	

Performance/Multi-CPU
In de huidige situatie presteert de firewall niet naar behoren. Er worden te veel resources (CPU-verbruik) gebruikt bij het aanzetten van de 'fail-over'. Het toevoegen van meerdere virtuele CPU's heeft geen nut, omdat het huidige besturingssysteem hier niet goed mee omgaat. Het nieuwe pakket dient compatibel te zijn met meerdere virtuele CPU's en dient maximaal voor 70% belast te kunnen worden bij intensieve routeringen en taken.

High Availability
Het uiteindelijke pakket dient bij uitval van de firewall alle verbindingen naar een back-up firewall te sturen. De verbindingen dienen met behoud van sessie-informatie overgezet te worden. Dit houdt in dat alle verbindingen hun informatie behouden en niet verbroken worden als de back-up firewall wordt ingezet bij een fail-over.

Beheerbaarheid/Automatisering
Omdat beheerbaarheid een belangrijk onderwerp is, dient de nieuwe firewall op verschillende manieren beheerd te kunnen worden. Zo moet het nieuwe pakket een web-interface hebben waarin er een visueel overzicht is van het netwerk en moet het pakket te automatiseren zijn. Dit houdt in dat er via scripts en commando's verschillende firewallregels aangepast kunnen worden en dat het pakket te beheren is zonder gebruik te maken van de web-interface.

Monitoring
Omdat het nieuwe pakket zorgt voor de beveiliging en het aanbieden van services (gateway/load-balacing/fail-over/DNS) voor de klantomgeving, dient het pakket zorgvuldig

gemonitord te worden. Dit kan gedaan worden door het pakket op te nemen in de huidige monitoring van het bedrijf. Hiermee kunnen de verschillende netwerken en services gemonitord worden. Meer hierover is te vinden in het hoofdstuk '*Monitoring*'.

IPv6 Routering
Omdat de IPv4-nummering langzamerhand opraakt, is de wens dat het nieuwe pakket compatibel is met IPv6. IPv6 is de opvolger van IPv4 en in een 'dual-stack' mode kan het pakket met beide protocollen omgaan.

VXLAN
VXLAN is de opvolger van het VLAN-protocol. Met het VLAN-protocol kunnen maximaal 4096 netwerken worden gemaakt. Omdat deze limiet tegenwoordig met Cloud-computing gemakkelijk behaald wordt, is de wens dat het nieuwe pakket het VXLAN-protocol ondersteunt. Met het VXLAN-protocol kunnen er ongeveer 16 miljoen netwerken gecreëerd worden.

Open source
Omdat het bedrijf veel met open source producten werkt, heeft het de wens dat de firewall ook open source is. Dit is niet noodzakelijk, vandaar dat dit als wens genoteerd is. Mocht er een betaald pakket zijn dat beter aan de eisen en wensen van het bedrijf voldoet, dan mag dit pakket geadviseerd worden.

Distributed firewall
Om de beveiliging van de services zo veilig mogelijk te houden, is de wens dat gedistribueerde firewallbeveiligingen toegevoegd kunnen worden op VM-niveau. Momenteel worden de beveiligingen op de traditionele manier op netwerkniveau gedaan. De wens van het bedrijf is om een extra laag beveiliging toe te voegen. Dit maakt het mogelijk om binnen een netwerk beveiligingen toe te passen op server/VM-niveau.

Quality of Service
Om bepaald verkeer voorrang te geven, is de wens dat de nieuwe firewall pakketten kan prioriteren, zodat er voorrang verleend kan worden aan een bepaalde verkeersstroom. Dit is als wens genoteerd, dus het is niet noodzakelijk dat het nieuwe pakket aan dit protocol moet voldoen.

Deze eisen en wensen zijn tot stand gekomen na een interview met de CTO van het bedrijf. Een overzicht van het interview ziet men in tabel 5;

TABEL 5; INTERVIEW EISEN EN WENSEN (DOBBELAAR, 2015)

Vraag	Antwoord/opmerking
Aan welke eisen dient de nieuwe firewall te voldoen?	Na overleg met Camiel Dobbelaar is de student samen met Camiel tot een aantal eisen/wensen gekomen. De eisen/wensen zijn als volgt: *Performance, High Availability, Beheerbaarheid, Automatisering, IPv6 Routering, VXLAN, Open-Source en Quality* en *Service*.
Wat is een goede test om de functionaliteit van de nieuwe firewall te testen?	Met het programma 'iPerf' kunnen er TCP-sessies worden opgezet. Het programma kan verschillende parallelle sessies opzetten; hierdoor kan de bandbreedte maximaal getest worden.
Wat dient er geautomatiseerd te kunnen worden?	De firewall rules moeten via een script automatisch ingevoerd kunnen worden. De beheerder hoeft dus niet op de firewall zelf in te loggen om rules aan te maken, dit dient automatisch te kunnen.
Wat wordt er verstaan onder beheerbaarheid?	De firewall dient firewall beheerbaar te zijn zonder een gebruikersinterface, waardoor automatisering mogelijk wordt.

6.2.5 Shortlist

De shortlist is een lijst waarop de pakketten vergeleken worden die het meest voldoen aan de eisen en wensen van het bedrijf. De shortlist is tot stand gekomen nadat de MoSCoW-analyse plaats heeft gevonden op de longlist. De longlist is weergegeven in het hoofdstuk '*Bijlagen – Onderzoeksrapport*' op pagina 94.

Uit de longlist is een aantal producten afgevallen, omdat deze niet aan alle wensen en eisen van het bedrijf voldoen.

Er zijn er drie producten uit de shortlist gekomen die aan de meeste eisen en wensen van de klant voldoen op basis van de MoSCoW-analyse. Deze producten zijn te zien in tabel 6.

TABEL 6; MOSCOW-ANALYSE OP PRODUCTEN

Product	High Availability (*Must*)	Performance	Centraal management (*Must*)	Automatisering (*Must*)	Open-source (*Should*)	IPv6 (*Should*)	Distributed firewall (Should)	VXLAN (*Should*)	QoS (*Could*)
pfSense	Ja	Ja	Ja	Ja/EasyRule	Ja	Ja	Nee	Ja	Ja
VMWare NSX	Ja	Ja	Ja	Ja/REST API's	Nee	Ja	Ja	Ja	Ja
Contrail	Ja	Ja	Ja	Ja/REST API's	Ja	Ja	Ja	Ja	Ja

De drie producten die in de shortlist staan worden meegenomen in het Proof of Concept. De student zal de drie producten in een testopstelling opbouwen en er zullen verschillende testen worden gedaan om te kijken welk product het beste past in de huidige omgeving van het bedrijf, een VMWare ESXi 5.5 omgeving. De pakketten zullen getest worden in de testomgeving die de student heeft gebouwd.

6.2.6 Kosten

In deze paragraaf zullen de kosten worden besproken die gekoppeld zijn aan de pakketten. Omdat niet alle pakketten 'closed-source' pakketten zijn, zullen er verschillen zijn in de kosten van de pakketten. De pakketten die in dit hoofdstuk besproken zullen worden zijn de pakketten die uit de shortlist zijn gekomen tijdens de onderzoeksfase. De pakketten zijn als volgt;

- pfSense
- VMWare NSX
- Contrail

Een overzicht van de kosten is te zien in tabel 7.

TABEL 7; KOSTEN PAKKETTEN SHORTLIST

Product	Kosten aanschaf	Kosten support
PfSense	€0,- (open source)	€0,- (community based support)
VMWare NSX	20 punten per beheerde VM*	Inbegrepen bij de aanschaf kosten
Contrail	€0,- (open source)	Aanvraag gedaan naar de kosten voor het support, maar de student heeft op het moment van schrijven nog geen antwoord op deze vraag gehad.

**Sentia heeft een VMWare licentiemodel van 5 punten per GB (RAM) per maand. Er wordt alleen gekeken naar het geheugen dat er in gebruik is. Als een machine bijvoorbeeld 4GB geheugen heeft, en er wordt maar 2 GB gebruikt, dan worden de kosten alleen over de 2GB berekend. Voor een NSX-installatie worden er 20 punten per maand gerekend per virtuele machine die in beheer is van het pakket(NSX). 1 punt is ongeveer 80 cent. Deze kosten zijn gebaseerd op de VMWare vCAN Guide 2015 Q2* (VMWare, VMware vCloud Air Network Program Product Usage Guide, 2015).

Omdat open source geen MUST is in de MoSCoW-analyse, vallen de pakketten waarvoor betaald moeten worden niet af. Op deze manier kan er een goede vergelijking worden gemaakt tussen de betaalde pakketten en de gratis pakketten.

6.2.7 Beantwoording deelvragen

In deze paragraaf zullen de deelvragen worden beantwoord. De deelvragen zijn beantwoord door middel van de onderzoeksresultaten, de literatuurstudie en het interview.

Deelvraag 1

Welke verschillen zijn er tussen een open source (gratis) firewall en een closed source (betaalde) firewall?

Om deze vraag te kunnen beantwoorden heeft de student onderzoek gedaan naar de verschillende pakketten die er in de shortlist staan. De shortlist maakt deel uit van de *onderzoeksfase*. In deze shortlist staan drie pakketten vermeld:

- pfSense (open source)
- VMWare NSX (closed source)
- Contrail (open source)

Na de literatuurstudie heeft de student de functies van de pakketten kunnen uittesten in een testomgeving. Het grootste verschil tussen een open source en een closed sourcepakket is de integratie van het betreffende pakket. De huidige infrastructuur van het bedrijf draait op een VMWare-omgeving. Het pakket wat VMWare zelf aanbiedt, NSX, heeft hierdoor een betere integratie dan de andere pakketten (pfSense en Contrail), die open source zijn.

PfSense en Contrail gaan anders om met de integratie van het pakket in de huidige infrastructuur. Bij VMWare NSX draait het pakket in de hypervisor en worden alle firewall-gerelateerde taken in de kernel (het hart) van de hypervisor uitgevoerd. Bij pfSense en Contrail worden deze taken uitgevoerd op een virtuele machine die deel uitmaakt van de hypervisor en dus niet geïntegreerd zit in de kernel van de hypervisor. Hierdoor worden firewall-gerelateerde taken op een andere manier uitgevoerd en kunnen deze taken meer resources vragen van de hypervisor. Dit houdt in dat verschillende functies die VMware NSX (closed source) aanbiedt door de andere twee pakketten niet uitgevoerd kunnen worden. Zo biedt VMware NSX de optie om beveiligingen toe te passen op VM-niveau. Dit betekent dat er beveiligingen geplaatst kunnen worden op de netwerkadapter van de virtuele machine. NSX maakt dit mogelijk omdat NSX geïntegreerd is in de kernel van de hypervisor en kennis heeft van de virtuele machines die hierop draaien.

Deelvraag 2

Welke firewallfuncties dienen er beschikbaar te zijn om aan de eisen van het bedrijf te voldoen?

Om de deelvraag zo goed mogelijk te beantwoorden heeft de student, na het uitvoeren van de literatuurstudie, een aantal interviews gehouden. Nadat de huidige situatie met de gewenste situatie was vergeleken, zijn er een aantal functies vastgesteld waaraan het nieuwe pakket hoort te voldoen, namelijk:

- Performance
- High Availability
- Beheerbaarheid
- Automatisering
- IPv6 Routering

- VXLAN
- Open source
- Distributed firewall
- Quality of Service

Deze functies dienen allemaal terug te komen in de functionaliteit van het pakket. Voor een uitgebreidere uitleg van de eisen, zie paragraaf 'Eisen en wensen' op pagina 25.

Deelvraag 3
Welke risico's zijn er bij het implementeren van een firewall in een bestaande omgeving?

Om deze vraag zo goed mogelijk te kunnen beantwoorden heeft de student een literatuurstudie uitgevoerd en verschillende praktijktesten gedaan in de testomgeving. Als de firewall in een productie-omgeving geïntegreerd zal worden, dan moeten de virtuele machines die in productie draaien verplaatst worden naar een andere fysieke machine. Op deze manier kan het netwerk opnieuw ingericht worden en kunnen de nieuwe beveiligingen toegepast worden. Omdat het migreren van de productie-omgeving niet zonder problemen verloopt, wordt er geadviseerd om de productiemachines eerst te klonen, zodat er een testomgeving wordt gecreëerd van de huidige productie-omgeving, en de migratie eerst uit te testen op de testomgeving die gekloond is vanuit de productie-omgeving.

Op deze manier kunnen de volgende risico's beperkt worden:

- Het uitvallen van de huidige firewall, waardoor communicatie met de virtuele machines niet meer mogelijk is.
- Het uitvallen van de services die het bedrijf aanbiedt aan haar klanten.
- Configuratieproblemen waardoor de huidige omgeving niet meer werkbaar is.

Deelvraag 4
Op welke manier wordt de firewall gemonitord?

Omdat het nieuwe pakket verschillende services aanbiedt aan klanten van het bedrijf, dient het pakket zorgvuldig gemonitord te worden. Monitoring kan op verschillende manieren gedaan worden. De firewall zal niet alleen gemonitord worden op up-time (of de firewall online is of niet) maar ook op de services en verschillende netwerken die de firewall aanbiedt voor de virtuele machines. Een overzicht van het ontwerp dat gecreëerd is voor de monitoring is te vinden in het hoofdstuk '*Bijlagen – Functioneel Ontwerp'* op pagina 124.

Deelvraag 5
Wat zijn de voor- en nadelen van een virtuele firewall ten opzichte van een fysieke firewall?

Deze vraag heeft de student kunnen beantwoorden door de literatuurstudie en door praktijktesten te doen. De functies van een firewall zijn niet beperkt als deze virtueel of fysiek draaien op een server. Het voordeel van virtualisatie is dat er meerdere (virtuele) machines en firewalls op een fysieke machine kunnen draaien. Dit is ook meteen het nadeel van virtualisatie. Omdat de verschillende virtuele machines op een fysieke machine draaien, worden de resources verdeeld over de virtuele machines. Als een firewall dus virtueel draait, dan zijn de resources beperkt ten opzichte van een fysieke machine waarop de firewall draait. De resources die gebruikt worden, zullen nooit optimaal gebruikt kunnen worden door de virtuele firewall.

Als er voor dezelfde firewall een virtuele installatie en een fysieke installatie gedaan wordt, met dezelfde (virtuele) hardware, dan zal de fysieke firewall beter presteren. Dit komt omdat de fysieke machine zich volledig kan richten op het uitvoeren van de firewalltaken.
Een virtuele firewall deelt zijn rekenkracht en andere resources met andere machines die virtueel draaien op een fysieke machine. Ook al is de firewall de enige virtuele machine op een fysieke server, dan nog zal de virtuele firewall minder presteren dan een fysieke firewall.

Sommige pakketten bieden de optie aan om de firewall te integreren in de kernel (het hart) van de hypervisor. Op deze manier heeft de firewall geen last van performance issues omdat de taken vanuit de kernel worden uitgevoerd en er geen virtuele machine nodig is die resources in beslag neemt.

6.3 Ontwerpfase

In deze paragraaf zullen de bevindingen van de ontwerpfase worden beschreven. De volledige documentatie van de ontwerpfase is te vinden in het hoofdstuk *"Bijlagen – Functioneel Ontwerp en Technisch Ontwerp"* op pagina 124 en 141.

6.3.1 Functioneel Ontwerp

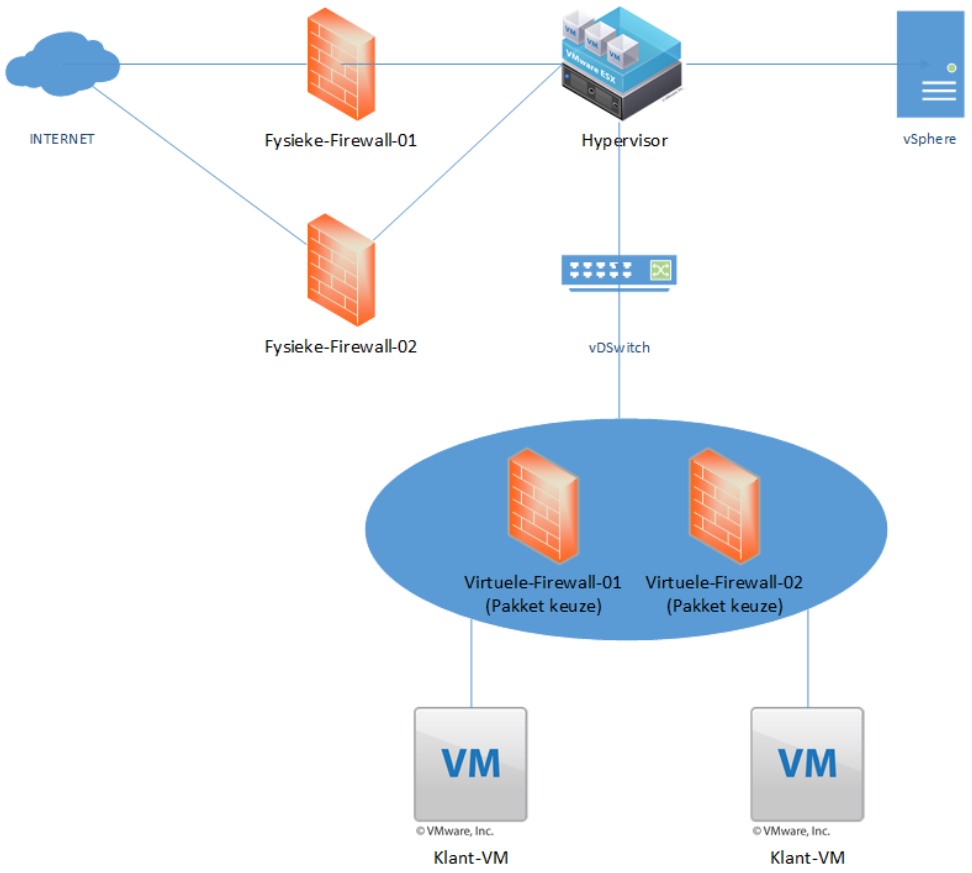
In deze paragraaf zullen de belangrijkste onderdelen van het Functioneel Ontwerp worden besproken. Deze paragraaf vormt de verslaglegging van de ontwerpfase.

6.3.2 Architectuur

In deze paragraaf zal de architectuur worden beschreven van het ontwerp dat gemaakt zal worden. Het ontwerp moet het mogelijk maken om aan de eisen en wensen te voldoen die in het hoofdstuk '*Eisen en wensen*' zijn genoemd.

Het doel van de architectuur is om een sjabloon te maken waarin het niet uitmaakt welk pakket er gekozen wordt. De architectuur is dus pakketonafhankelijk.

Een overzicht van de architectuur is te zien in afbeelding 8.



AFBEELDING 8; ARCHITECTUUR

De architectuur bestaat uit verschillende componenten die het mogelijk maken om aan de eisen en wensen van het bedrijf te voldoen. De beschrijving van deze componenten is te vinden in het hoofdstuk '*Bijlagen – Functioneel Ontwerp – Architectuur*' op pagina 124.

6.3.3 Beheerontwerp

Om het pakket te beheren heeft de student een beheerontwerp gemaakt. In dit beheerontwerp is vastgelegd hoe men een verbinding kan maken met de firewall en op welke manier de firewall te beheren is. Voor een volledig overzicht van het beheerontwerp, zie het hoofdstuk *'Bijlagen – Functioneel Ontwerp – Beheerplan'* op pagina 124.

Eisen beheer

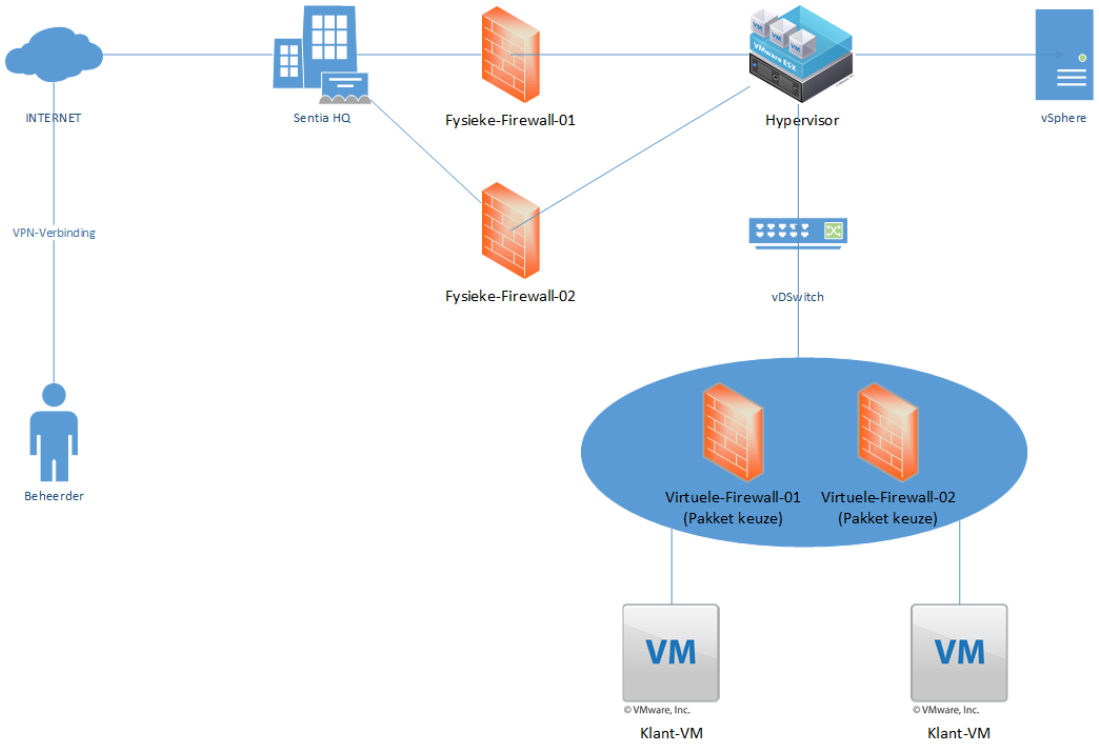
Het beheer dient aan een aantal eisen te voldoen:

- Beheer via de interface van het pakket; hierdoor is een visueel overzicht mogelijk van het netwerk.
- Beheer via automatisering. Het beheer moet geautomatiseerd worden; hierdoor is het mogelijk om verschillende aanpassingen te doen aan het pakket zonder in te loggen op de (web)interface van het pakket. Aanpassingen dienen via bijvoorbeeld een script doorgevoerd te kunnen worden.

- Het pakket dient een overzicht te hebben van alle netwerken en, indien er ingelogd wordt met het ‘administrator’-account, dienen alle netwerken beheerd te kunnen worden.
- Het pakket dient beheerbaar te zijn voor verschillende netwerken. Dit houdt in dat er bijvoorbeeld beheer gedaan kan worden voor een apart netwerk op de firewall. Als bijvoorbeeld netwerk A en B zijn aangemaakt op de firewall, dan dienen de firewallinstellingen voor netwerk A en netwerk B afzonderlijk van elkaar beheerd te kunnen worden. Op deze manier wordt ervoor gezorgd dat de beheerder van netwerk A niet bij de firewall van netwerk B kan.

Overzicht beheer

In deze paragraaf zal het overzicht van het beheer worden geschetst. Het overzicht is te zien in afbeelding 9.



AFBEELDING 9; OVERZICHT BEHEER

De beheerder logt in via een VPN-verbinding via het internet op een van de kantoren van het bedrijf. Als de beheerder eenmaal ingelogd is, kan de beheerder via de VPN het pakket managen.

6.3.4 Technisch Ontwerp

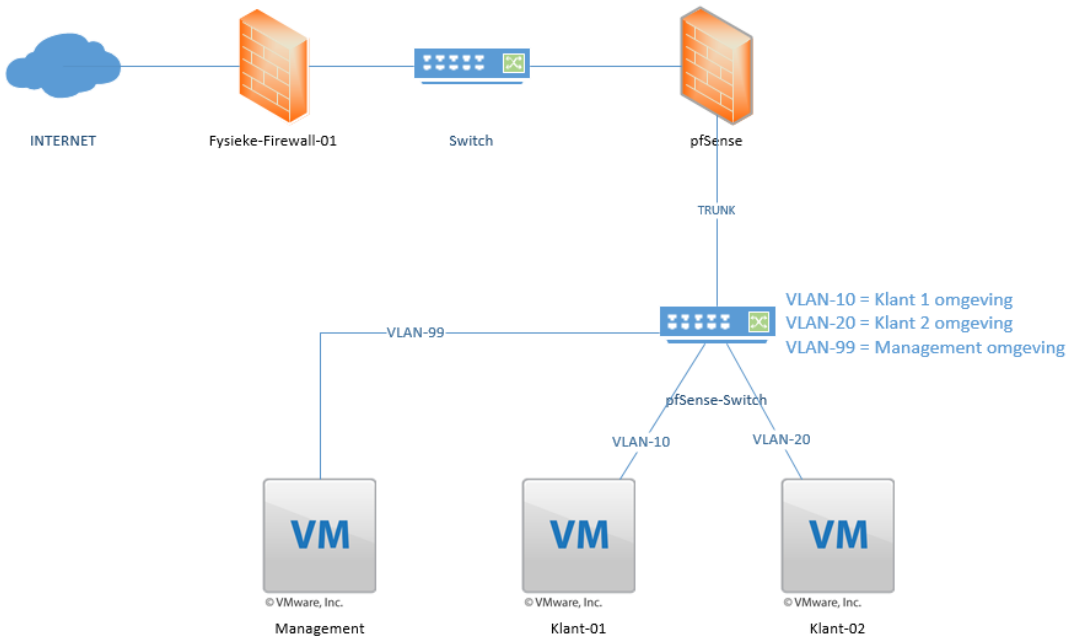
In deze paragraaf zullen de belangrijkste onderdelen van het Technisch Ontwerp worden besproken. Voor het volledige Technisch Ontwerp, zie het hoofdstuk '*Bijlagen – Technisch Ontwerp*' op pagina 141.

Omdat er drie pakketten zijn geadviseerd in de shortlist, zijn er drie technische ontwerpen gemaakt. De technische ontwerpen zullen in dit hoofdstuk worden weergegeven.

pfSense

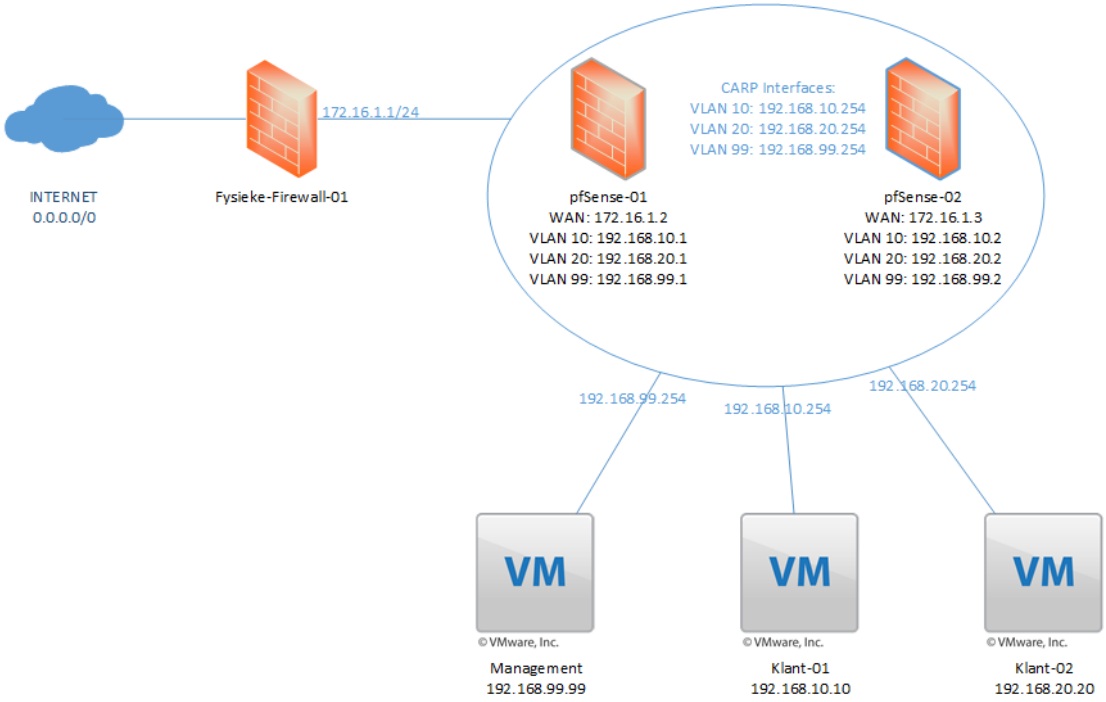
De eerste omgeving die de student heeft onderzocht is de pfSense-omgeving. De pfSense-omgeving gaat met de netwerken om op de 'traditionele manier' en is geen SDN controller. Met 'traditionele manier' wordt er bedoeld dat de netwerken door één firewall beheerd worden en dat de netwerkbeveiligingen op netwerkniveau plaatsvinden. Machines in hetzelfde netwerk hebben dus dezelfde rechten. Om een scheiding te maken tussen de laag 2 en laag 3 componenten zijn er twee ontwerpen gemaakt, één voor laag 2 en één voor laag 3.

Het ontwerp voor laag 2 is te zien in afbeelding 10.



AFBEELDING 10; LAAG-2 ONTWERP PFSENSE

Om een logische netwerktekening te creëren is er ook een laag 3 ontwerp gemaakt van de pfSense-omgeving. In deze tekening zijn de IP-adresseringen zichtbaar en wordt er duidelijk gemaakt hoe de communicatie plaatsvindt. Het ontwerp voor laag 3 is te zien in afbeelding 11.



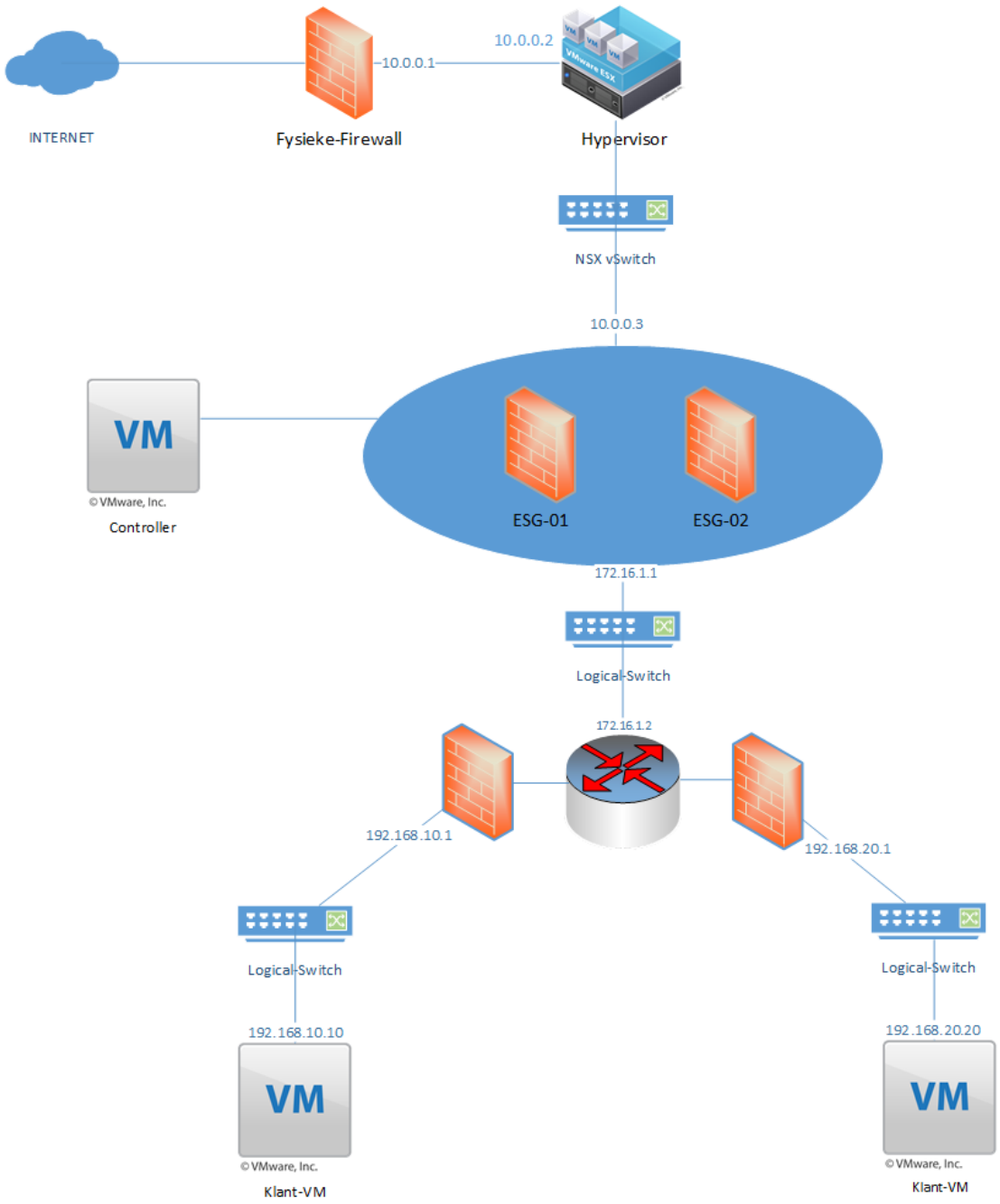
AFBEELDING 11; LAAG 3 ONTWERP PFSENSE

Voor de volledige technische specificaties van de pfSense omgeving, zie het hoofdstuk '*Bijlagen – Technisch Ontwerp'* op pagina 141.

VMware NSX

Het tweede pakket dat de student onderzocht heeft is VMware NSX. NSX gaat anders om met de netwerken dan op de 'traditionele' manier. NSX heeft een controller waarmee de verschillende netwerken beheerd kunnen worden. Ook kunnen de netwerken apart beheerd worden via de betreffende firewall.

Omdat de hypervisor op VMWare ESXi draait en NSX van hetzelfde bedrijf is, wordt de firewall geïntegreerd in de hypervisor. Op deze manier heeft de firewall kennis van de virtuele machines die draaien op de hypervisor en kunnen de beveiligingen direct op VM-niveau worden uitgevoerd. Het ontwerp van de NSX-omgeving is te zien in afbeelding 12.



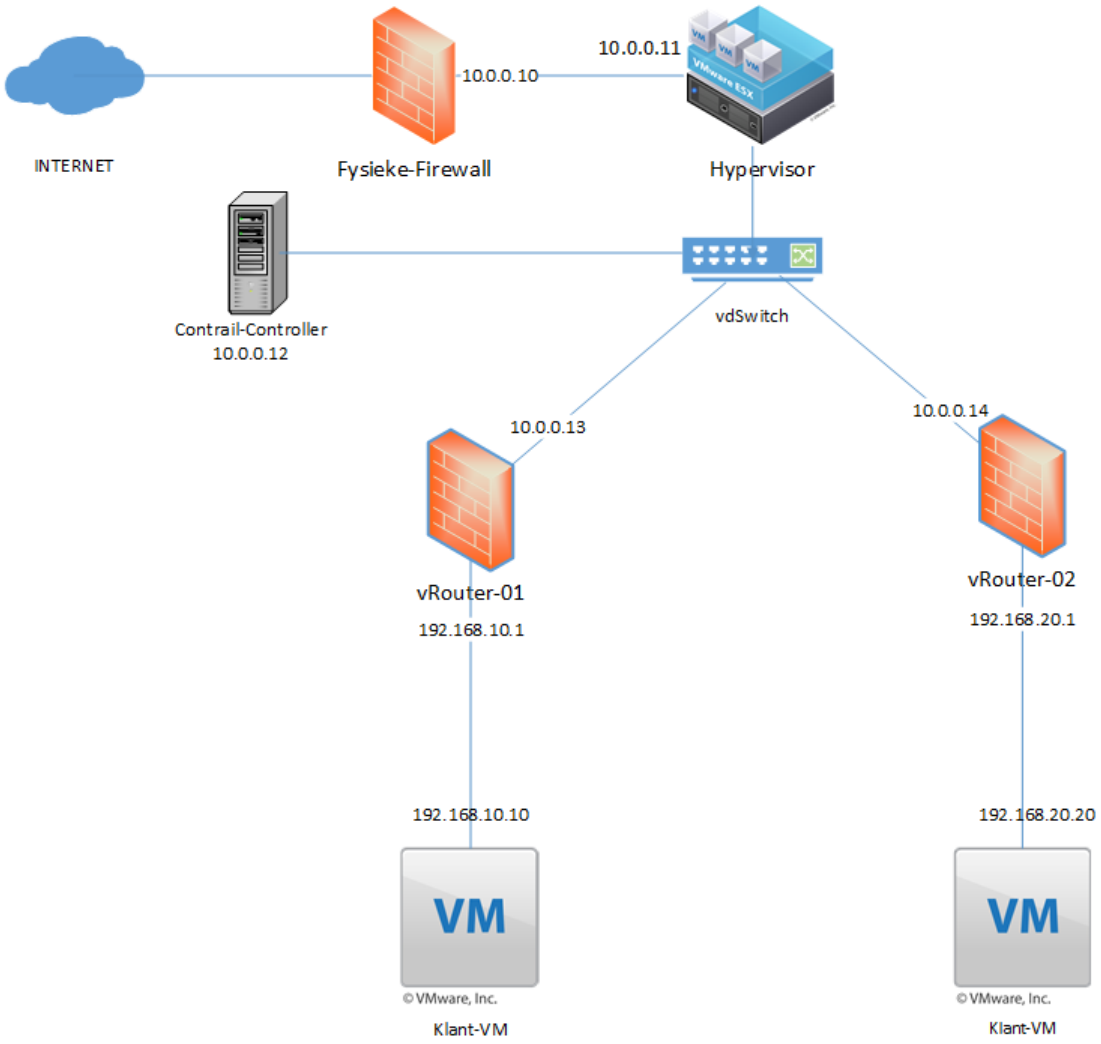
AFBEELDING 12; ONTWERP NSX OMGEVING

Omdat NSX de laag 2 en laag 3-componenten samenvoegt (waardoor routering op laag 2 mogelijk wordt) zijn de componenten in dezelfde tekening getekend. Op deze manier wordt een duidelijk overzicht gecreëerd van hoe de netwerkcomponenten met elkaar communiceren.

Voor het volledige technisch ontwerp, zie het hoofdstuk '*Bijlagen – Technisch Ontwerp*' op pagina 141.

Contrail

Het derde pakket dat de student heeft onderzocht is het pakket Contrail. Contrail is een open sourcepakket en gaat met de netwerken om op de 'traditionele' manier. Dit komt omdat de Contrail firewall niet geïntegreerd is in de hypervisor. De firewall wordt op een aparte virtuele machine geïnstalleerd en maakt gebruikt van de virtuele resources die toegekend zijn aan de firewall. Omdat Contrail een SDN controller heeft kunnen de firewalls en netwerken via deze controller beheerd worden. De netwerken kunnen ook beheerd worden via de betreffende firewall. Een overzicht van het ontwerp van het pakket Contrail is te zien in afbeelding 13.



AFBEELDING 13; ONTWERP CONTRAIL OMGEVING

Omdat Contrail laag 2 en laag 3-protocollen met elkaar combineert, zijn de netwerkcomponenten in dezelfde tekening getekend. Voor een volledig overzicht van het technisch ontwerp, zie het hoofdstuk '*Bijlagen – Technisch Ontwerp*' op pagina 141.

6.4 Validatiefase

Tijdens deze fase is er samen met de student en bedrijfsbegeleider gekeken naar de geadviseerde pakketten en de gecreëerde ontwerpen (functioneel en technisch). De pakketten van de shortlist en de ontwerpen voldeden aan de eisen en wensen van het bedrijf. Daarom heeft de student akkoord gekregen om door te gaan naar de volgende fase, de *implementatiefase*.

6.5 Implementatiefase

In deze paragraaf zullen de bevindingen van de implementatie worden beschreven. De volledige documentatie van de implementatiefase is te zien in het hoofdstuk *"Bijlagen – Testplan en Proof of Concept"* op pagina 156 en 163.

6.5.1 Testplan

In deze subparagraaf zal worden beschreven hoe de geadviseerde pakketten getest worden. De pakketten zullen alle drie op dezelfde manier worden getest. De pakketanalyse wordt uitgevoerd met het programma 'iPerf'. IPerf is een programma dat het mogelijk maakt om de maximale bandbreedte van een (virtuele) machine te benutten.

Omdat de gekozen pakketten firewalls betreffen, wordt routing ook ondersteund. De manier van testen gebeurd door twee machines in verschillende netwerken met elkaar te laten communiceren middels het programma iPerf. De firewall (het geadviseerde pakket(ten)) zorgt dan voor de routering. De performance van het betreffende pakket kan dan worden gemonitord om te kijken hoe het pakket presteert onder deze omstandigheden.

Testomgeving

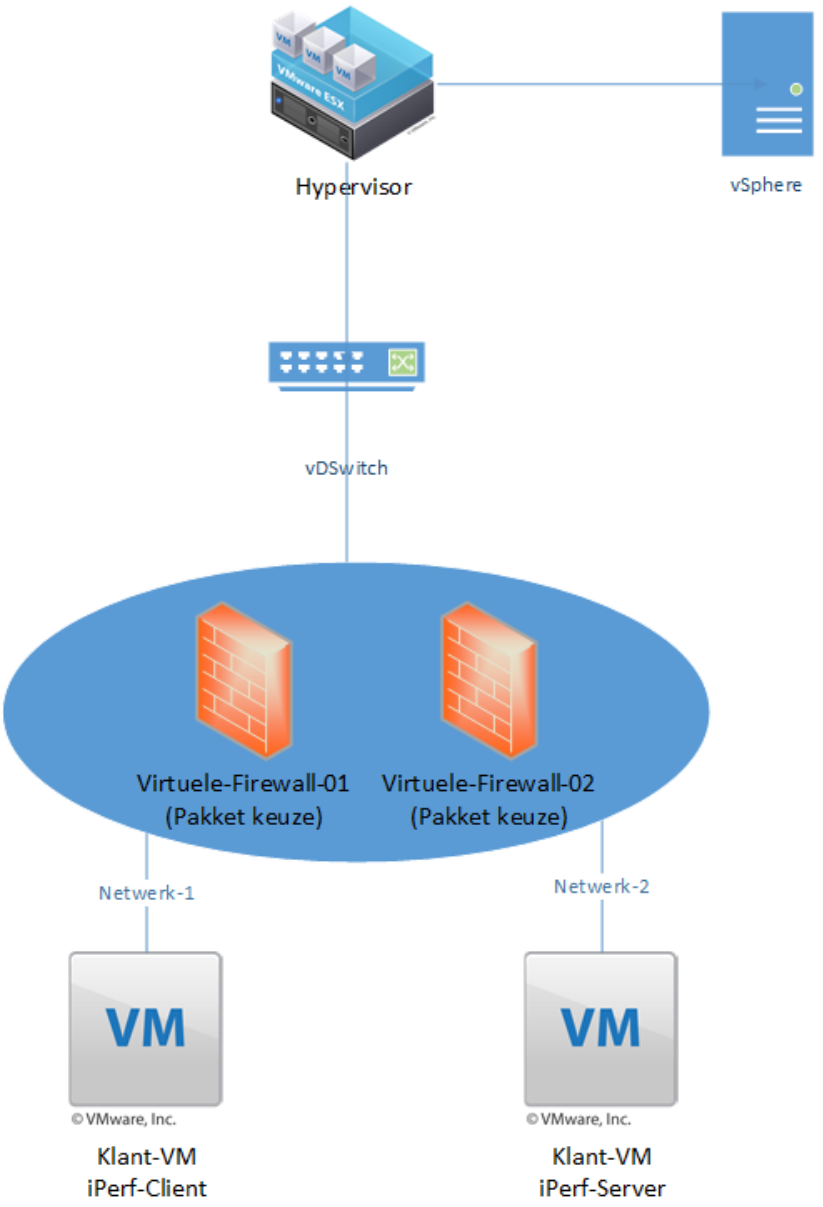
Omdat het onderzoek en het testen niet in een productie-omgeving plaats kunnen vinden, heeft de student een testopstelling gecreëerd. De testopstelling bestaat uit een fysieke machine. Deze machine simuleert de VMware ESXi 5.5-omgeving waarop de omgeving van de klanten draait.

Om de testresultaten zo veel mogelijk hetzelfde te houden als in de productie-omgeving, heeft de student ervoor gekozen om de productie-omgeving na te bouwen als een testomgeving. De VMWare ESXi 5.5-machine is de hypervisor. Hierop draait dezelfde software als in de productie-omgeving.

Op deze manier kan de student het netwerk ongeveer hetzelfde houden en worden de testresultaten niet beïnvloed door een softwareconflict.

Op de VMWare ESXi 5.5-machine draaien twee virtuele machines. Deze virtuele machines staan elk apart in een ander netwerk; dit simuleert de verschillende klantomgevingen.

Het is aan de student om te onderzoeken welke virtuele firewall het beste presteert in een virtuele omgeving en welke type virtuele firewall het beste presteert in de bestaande infrastructuur past. Afbeelding 14 toont een netwerktekening van de testomgeving die de student gecreëerd heeft.



AFBEELDING 14; TESTOMGEVING

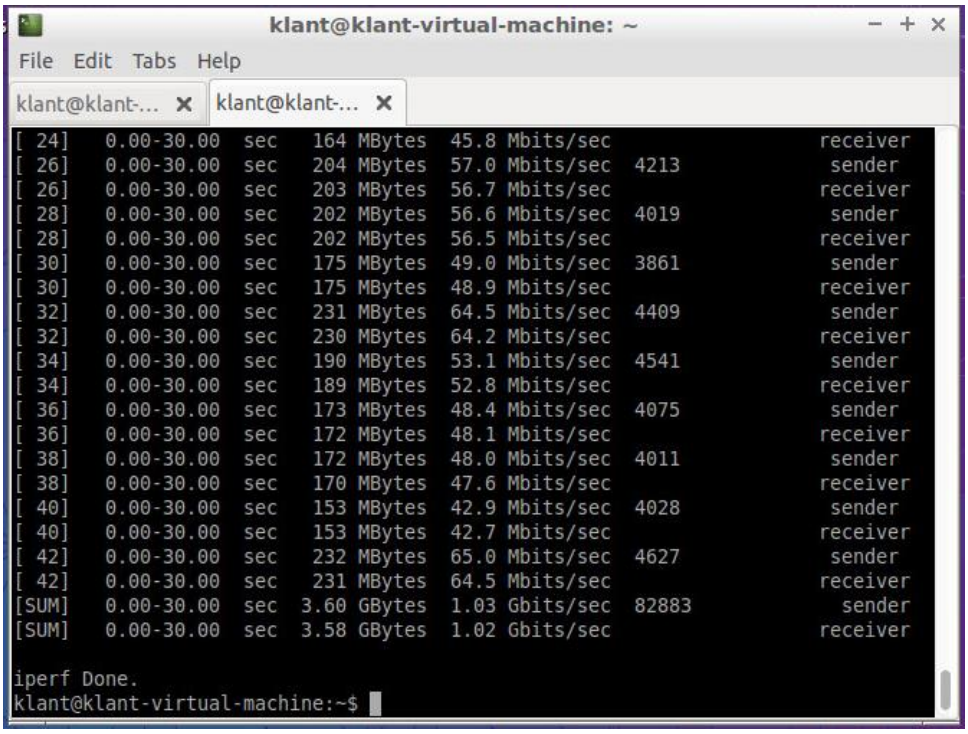
6.5.2 Proof of Concept

In deze paragraaf bevindt zich de verslaggeving van het Proof of Concept. De pakketten zijn getest qua functionaliteit op de performance die de pakketten leveren bij een routering van 1 GB per seconde. Er is gekeken hoe de pakketten reageren op de geschetste situatie en de bevindingen zijn gedocumenteerd in deze paragraaf. De pakketten worden alle drie op dezelfde manier getest.

pfSense

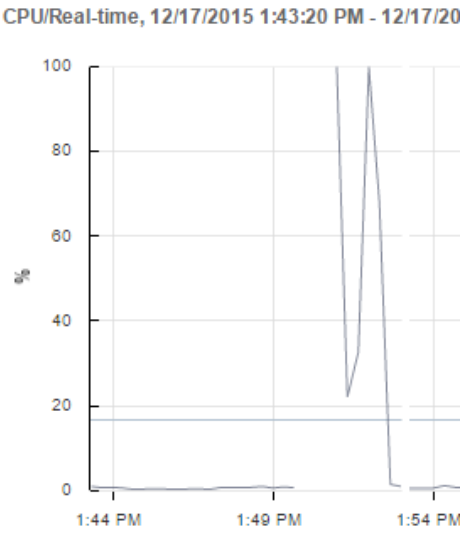
In afbeelding 15 ziet men een test die gedaan is tussen twee virtuele machines in twee

verschillende netwerken. Om communicatie tussen de netwerken mogelijk te maken, wordt er gebruikgemaakt van de interne routingfunctie van het pakket.



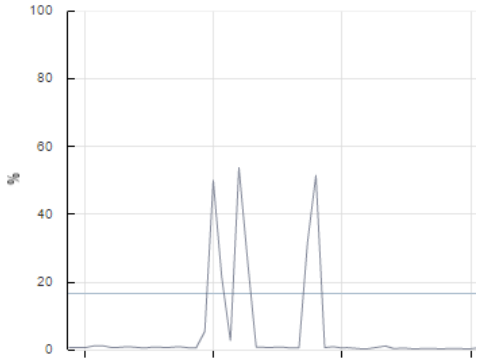
AFBEELDING 15; IPERF PFSENSE

Zoals te zien in afbeelding 15, wordt er een maximale bandbreedte van 1,03 Gbit per seconde gehaald. Tijdens de test is het CPU-verbruik (met een enkele CPU) gemonitord. De resultaten hiervan zijn te zien in afbeelding 16.



AFBEELDING 16; 100% CPU-BELASTING

In afbeelding 16 kan men zien dat de CPU van de firewall voor 100% werd verbruikt tijdens de ‘iPerf’ test. Na het toevoegen van meerdere CPU’s is de ‘iPerf’ test nogmaals gedaan. De resultaten hiervan zijn te zien in afbeelding 17.



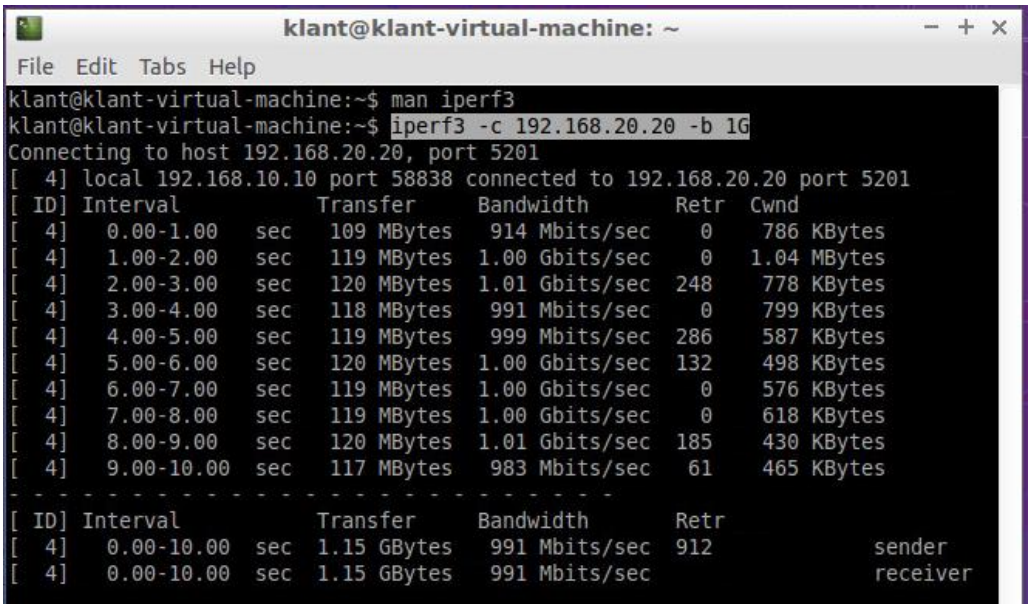
AFBEELDING 17; 53% CPU-BELASTING

Na het toevoegen van meerdere CPU’s werd het CPU-verbruik bij een maximale belasting van 1 GBit per seconde 53%.

Het operating-system van pfSense gaat dus goed om met het toekennen van meerdere CPU’s en de belasting wordt verdeeld tussen de CPU’s.

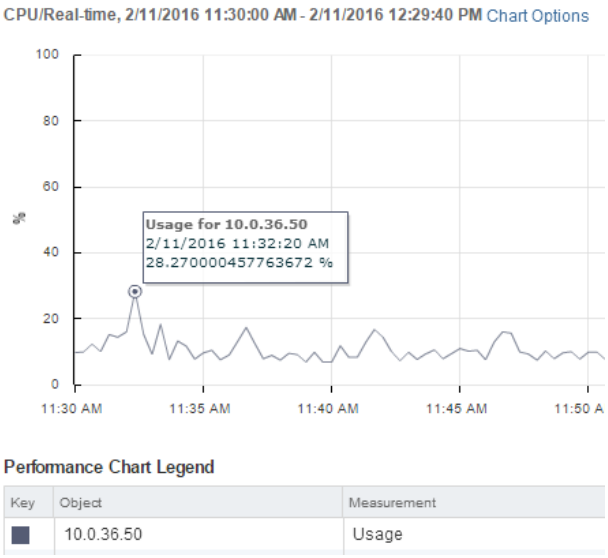
VMWare NSX

In afbeelding 18 is te zien dat er verbinding wordt gemaakt met een machine in netwerk 20 (192.168.20.20). De bronmachine zit in het netwerk 10 (192.168.10.10). Om de communicatie plaats te laten vinden moet er dus gerouteerd worden door de firewall en moeten de iPerf-verbindingen ook gerouteerd worden. In afbeelding 18 is te zien dat er 1 GB per seconde gerouteerd wordt van de ene machine naar de andere machine.



AFBEELDING 18; IPERF NSX

Omdat NSX geïntegreerd zit in de hypervisor, wordt de routering niet door de firewall gedaan maar door de hypervisor zelf. Dit komt doordat de firewall de kernel van de hypervisor direct kan aanspreken en hiervoor geen eigen (virtuele) resources hoeft te gebruiken. Dit heeft als voordeel dat het weinig performance kost om de routering plaats te laten vinden, zoals te zien in afbeelding 19.

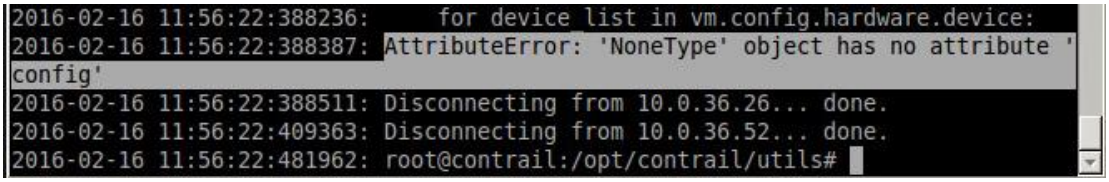


AFBEELDING 19; CPU-VERBRUIK NSX

Zoals afgebeeld wordt de CPU bij een routering van 1 GB per seconde voor maximaal 28,27% belast. De reden dat de CPU een lage belasting heeft, is dat de firewall direct wordt aangesproken in de kernel van de hypervisor.

Contrail

De student heeft vele malen geprobeerd om de integratie met de huidige omgeving werkend te krijgen. Helaas is dit niet gelukt. Tijdens het installeren loopt het script vast op de volgende error, zie afbeelding 20.



AFBEELDING 20; CONTRAIL ERROR

De student heeft geprobeerd om de gehele omgeving opnieuw te installeren in de hoop de installatie van het pakket Contrail werkend te krijgen. Helaas is dit niet gelukt. De student kan concluderen dat het pakket nog niet volledig werkend te krijgen is in een vCenter 5.5-omgeving. Ook ziet de student dat er in de scripts kleine foutjes zitten, waardoor duidelijk wordt dat het pakket nog niet helemaal klaar is voor productie in combinatie met een vCenter-omgeving.

7 Conclusie

In dit hoofdstuk zal het advies van de student worden gegeven. Ook de hoofdvraag van het onderzoek zal in dit hoofdstuk worden beantwoord.

De hoofdvraag is als volgt geformuleerd: *"Welk type firewall voldoet het meest aan de gestelde eisen van het bedrijf en is het meest geschikt voor de huidige infrastructuur?"*

Om de hoofdvraag zo goed mogelijk te beantwoorden zijn er een literatuurstudie, een interview en praktijktesten gedaan. De verschillende firewalls in de short list op pagina 28 zijn met elkaar vergeleken en op basis van deze onderzoeken kan de hoofdvraag als volgt worden beantwoord.

Een gedistribueerde stateful firewall past het beste in de huidige infrastructuur. Dit is een combinatie van een stateful firewall en een gedistribueerde firewall. Meer hierover is te zien in de paragraaf *'Theoretisch Kader'* op pagina 21.

Omdat de huidige omgeving op een VMWare ESXi 5.5-hypervisor draait en uit verschillende testen is gebleken dat VMWare NSX het best presteert en integreert in de huidige omgeving, geeft de student het advies deze firewall te gebruiken. De vraagstelling van het onderzoek was om te achter te komen wat de 'best' mogelijke backend firewall is voor de huidige omgeving.

VMware NSX integreert direct op kernelniveau met de hypervisor. Hierdoor worden firewall-gerelateerde taken direct op de kernel uitgevoerd en maakt de firewall gebruik van de fysieke resources van de hypervisor. De andere twee firewalls, pfSense en Contrail, maken gebruik van een aparte virtuele machine. Firewall-gerelateerde taken maken dan gebruik van de virtuele resources van deze virtuele machine. Zoals te zien is in afbeelding 17 op pagina 43 wordt in de pfSense-omgeving de CPU voor 53% belast bij een routering van 1 GB per seconde.

De CPU-belasting van VMware NSX bij een routering van 1 GB per seconde ligt op 28,3%. Het drastische verschil tussen 53% en 28,3% wordt mogelijk gemaakt door de werking en integratie van VMware NSX met de huidige omgeving.

Omdat VMware NSX zich direct op de hypervisor integreert, heeft de firewall kennis van alle virtuele machines die er op hypervisor draaien. Het voordeel hiervan is dat er beveiligingen geplaatst kunnen worden per virtuele machine. Normaal worden beveiligingen op netwerk (VLAN) niveau gedaan. Twee machines in hetzelfde netwerk hebben dan dezelfde beveiligingen. Met VMWare NSX is het mogelijk om twee machines in hetzelfde netwerk aparte beveiligingen te gegeven. Ook al zitten de twee machines in hetzelfde netwerk, dan kunnen de beveiligingen alsnog per virtuele machine worden ingesteld.

Dit type firewall is een combinatie van een stateful firewall en een gedistribueerde firewall, wat meteen het antwoord op de hoofdvraag geeft.

Voor het beheren van de firewall heeft de student een beheerontwerp gecreëerd. Via een VPN-verbinding wordt er verbinding gemaakt met één van de hoofdkantoren van het bedrijf. Zie

´Bijlagen – Functioneel Ontwerp – Beheerontwerp' voor het gehele ontwerp. Dit ontwerp maakt het mogelijk om de firewall te beheren.

De kosten van VMware NSX worden door middel van punten geregeld. Per beheerde machine kost VMware NSX 20 punten. Eén punt staat ongeveer gelijk aan €0,80. Worden er dus bijvoorbeeld drie machines beheerd door VMware NSX, dan zijn dit 60 punten, wat ongeveer gelijk staat aan €48,- voor de drie beheerde machines.

Om deze redenen geeft de student het bedrijf Sentia het advies om het product VMware NSX te gebruiken.

7.1 Aanbevelingen

In deze paragraaf zullen de aanbevelingen worden beschreven die de student wil meegeven aan het bedrijf.

Implementatie
Indien het bedrijf het geadviseerde pakket wil integreren in de huidige omgeving, is het verstandig om een implementatieplan te maken. In dit plan moet worden beschreven hoe de implementatie van het pakket zal worden uitgevoerd.

Om de implementatie zo goed mogelijk uit te voeren geeft de student als advies mee om de virtuele machines in de huidige infrastructuur eerst gedeeltelijk of per cluster te klonen naar een testmachine.

Als de betreffende machines eenmaal gekloond zijn, kan VMware NSX geïnstalleerd worden op de testmachine en kunnen de verschillende beveiligingen worden overgenomen van de huidige firewall naar het nieuwe pakket VMware NSX.

Afhankelijk van het aantal machines dat beveiligd moeten worden, kan het creëren van een testomgeving ongeveer één à twee weken duren. Na deze periode kunnen er verschillende testen worden uitgevoerd in de testomgeving en kan er worden bekeken welke machines beheerd moeten worden door VMware NSX.

Als het testen voltooid is, kunnen de machines die gekloond waren gemigreerd worden naar de productieomgeving. Het migreren kan 'live' gebeuren met het programma vMotion. vMotion is een techniek die het mogelijk maakt om virtuele machines live (zonder de machines uit te schakelen) te migreren naar een andere host, zonder downtime van de virtuele machines. vMotion is beschikbaar in de huidige infrastructuur en maakt deel uit van de VMWare-omgeving. Op deze manier kan de testomgeving gemigreerd worden naar de productieomgeving.

IP-adressering
Omdat het pakket NSX de beveiligingen per virtuele machine kan toepassen, is het mogelijk om verschillende klanten in hetzelfde sub-net te plaatsen. Zo kunnen er dus bijvoorbeeld meerdere klanten in het 192.168.1.0/24-netwerk zitten. Deze klantomgevingen kunnen van elkaar beschermd worden door de beveiligingen toe te passen op VM-niveau. VM's in hetzelfde netwerk kunnen dus beveiligd worden tegen elkaar. Op deze manier kunnen er grotere sub-nets worden gebruikt zonder dat de security hieronder lijdt.

Kosten
Om de kosten in kaart te brengen voor het pakket VMware NSX zal de student de kosten berekenen voor een standaard klantomgeving. Een standaard klantomgeving bestaat uit de volgende drie onderdelen: een webserver, een databaseserver en een applicatieserver. Om het verkeer naar buiten te regelen wordt er gebruikgemaakt van een ESG-router. Op de ESG-router kunnen verschillende klantomgevingen worden aangesloten. De klantomgevingen worden onderscheiden door de DLR-router. De DLR regelt het verkeer tussen de VM's. De ESG-router is

dus noodzakelijk voor het routeren naar buiten. De kosten voor deze ESG-router zijn 20 punten, wat ongeveer gelijk staat aan €16,-. Per ESG zijn er tien klantomgevingen aan te sluiten.

In totaal zijn er dus vier virtuele machines per klantomgeving (de ESG hoort niet bij een standaard klantomgeving). Per VM wordt er 20 punten per maand berekend. Voor een standaard klantomgeving is het bedrijf dan 20 punten maal 4 = 80 punten per maand kwijt, wat omgerekend uitkomt op ongeveer €64,- per maand.

Deze kosten komen boven op de standaardkosten die Sentia betaalt voor de huidige VMware-licentie.

High Availability

Om de omgeving altijd bereikbaar te houden maakt VMware NSX gebruik van de NSX vSwitch. De NSX vSwitch heeft kennis van alle routeringen die plaatsvinden binnen de NSX-omgeving. Bij uitval van de ESG of de DLR kan de NSX vSwitch ervoor zorgen dat de routering alsnog plaats kan vinden. Omdat het motto van Sentia *"Driven by Continuity"* is - het bedrijf wil de services dus een zo hoog mogelijke continuïteit geven - adviseert de student om de ESG en de DLR-routers alsnog dubbel uit te voeren. Mocht er iets misgaan met de NSX vSwitch tijdens het overschakelen tussen een uitgevallen router, dan kan de redundante ESG en/of DLR deze taken alsnog op zich nemen. In deze situatie wordt de fail-over gedaan door de redundante ESG/DLR.

Mocht de ESG/DLR om wat voor reden dan ook niet kunnen overschakelen naar de andere actieve router, dan zorgt de NSX vSwitch voor de routering. Op deze manier blijven de services die het bedrijf aanbiedt aan haar klanten altijd bereikbaar.

8 Procesevaluatie

In het begin van het afstudeerproces heeft de student een afstudeervoorstel opgesteld. In dit afstudeervoorstel heeft de student beschreven hoe hij het project denkt aan te pakken. Er is een (tijdelijke) planning gemaakt en in deze planning zijn de verschillende fases opgenomen die tijdens het project doorlopen zouden worden. De fases die in het afstudeervoorstel waren beschreven, zijn

- Onderzoeksfase
- Ontwerpfase
- Validatiefase
- Documentatiefase

De student heeft de initiatiefase niet vermeld in het afstudeervoorstel. Het afstudeervoorstel maakt deel uit van de initiatiefase.

Na de goedkeuring van het afstudeervoorstel door de examencommissie van de Hogeschool Utrecht heeft de student een Plan van Aanpak geschreven. In dit Plan van Aanpak is samen met de bedrijfsbegeleider gekeken of de aanpak van het project reëel was en of de geplande fases zouden leiden tot de resultaten die het bedrijf wenst van de student. Het Plan van Aanpak maakte deel uit van de onderzoeksfase.

Nadat het Plan van Aanpak was goedgekeurd door het bedrijf en de Hogeschool Utrecht, kon de student beginnen met het onderzoek. De student heeft een onderzoeksrapport opgesteld waarin verschillende literatuurstudies en een interview verwerkt waren. Op deze manier heeft de student de eisen en wensen van het bedrijf in kaart weten te brengen en heeft hij een beter beeld gekregen wat het bedrijf van hem verwachtte. Het onderzoeksrapport maakte deel uit van de onderzoeksfase.

Nadat het onderzoeksrapport afgerond was, heeft de student een Functioneel Ontwerp gemaakt waarin beschreven stond aan welke functies het nieuwe pakket moest voldoen. In dit Functioneel Ontwerp heeft de student een architectuur ontworpen waarin duidelijk gemaakt wordt waarvoor de functionele eisen en wensen dienen. Het Functioneel Ontwerp maakte deel uit van de ontwerpfase.

Na het afronden van het Functioneel Ontwerp heeft de student verschillende technische ontwerpen gemaakt voor de verschillende pakketten. Gedurende het maken van deze ontwerpen heeft de student een beter inzicht gekregen van de pakketten en heeft hij de ontwerpen met elkaar vergeleken om zo een beeld te krijgen van hoe de verschillende pakketten omgaan met de verschillende functionaliteiten. Het Technisch Ontwerp maakte deel uit van de ontwerpfase.

Nadat de ontwerpen waren gemaakt, werd samen met de bedrijfsbegeleider gekeken naar de gemaakte ontwerpen en werd duidelijk dat er nog een aantal dingen aangepast moesten worden. Toen de student deze aanpassingen gemaakt had, werden deze gevalideerd tijdens de

validatiefase. In de validatiefase werden het Functioneel Ontwerp en de verschillende technische ontwerpen bekeken; na akkoord kon doorgegaan worden naar de implementatiefase.

Tijdens de implementatiefase heeft de student de testopstelling beschreven die hij gemaakt heeft en heeft hij de testresultaten van de verschillende pakketten gedocumenteerd. Na deze fase werd al snel duidelijk dat er maar één pakket uit de shortlist voldeed aan alle eisen en wensen van het bedrijf, namelijk VMware NSX. Na deze fase is de student doorgegaan naar de documentatiefase.

In de documentatiefase werden alle bevindingen van de student beschreven in de scriptie. De scriptie is een samenhang van alle deelproducten die tijdens de faseringen gemaakt zijn.

Terugkijkend naar het afstuderen vindt de student dat de planning redelijk overeenkomt met wat hij in gedachten had. Toen de student begon bij het bedrijf, heeft hij meteen een testomgeving opgezet om zo de theorie van de literatuurstudie in de praktijk te zien. Dit heeft veel geholpen tijdens de onderzoeksfase en hierdoor, samen met het interview, heeft de student de eisen en wensen van het bedrijf weten te achterhalen.

Bibliografie

B.V, S. (2015). *Virtual Network.* Nieuwegein: Sentia B.V.

Bannai, V. (2013, 11 11). *slideshare*. Opgehaald van slideshare.net: http://www.slideshare.net/vbannai/sdn-presentation-bbffinal

Elsherbeny, A. M. (2014, 05 07). *what-is-the-difference-between-stateless-and-statefull-firewall/*. Opgehaald van Bayt.com: http://www.bayt.com/en/specialties/q/43242/what-is-the-difference-between-stateless-and-statefull-firewall/

FAQs (2013, 03 12). *Firewall*. Opgehaald van FAQs: http://www.faqs.org/faqs/firewalls-faq/

Greene, T. (2014, 02 02). *the-evolution-of-application-layer-firewalls*. Opgehaald van networkworld.com: http://www.networkworld.com/article/2330057/network-security/the-evolution-of-application-layer-firewalls.html

IdemDito (2005, 03 12). *OSI Model*. Opgehaald van TCP: http://server.idemdito.org/svt/techtalk/osi.htm

informIT (2005, 02 08). *Stateful Firewalls*. Opgehaald van informit.com: http://www.informit.com/articles/article.aspx?p=373120

NetworkComputing (2012, 08 04). *networkcomputing*. Opgehaald van networkcomputing.com: http://www.networkcomputing.com/networking/7-essentials-software-defined-networking/1587046750

Onisick, J. (2013, 06 19). *definethecloud*. Opgehaald van definethecloud.net: http://www.definethecloud.net/network-abstraction-and-virtualization-where-to-start/

OpenNetworking (2015, 08 02). *opennetworking*. Opgehaald van opennetworking.org: https://www.opennetworking.org/sdn-resources/sdn-definition

Revelle, D. (2011, 04 05). *usenix.* Opgehaald van usenix.org: https://www.usenix.org/system/files/login/articles/105498-Revelle.pdf

SDXcentral (2015, 04 08). *sdxcentral*. Opgehaald van sdxcentral.com: https://www.sdxcentral.com/resources/nfv/whats-network-functions-virtualization-nfv/

Sysadmintutorials (2006, 01 03). *Sysadmintutorials*. Opgehaald van VMWare ESXI: http://www.sysadmintutorials.com/tutorials/vmware-vsphere-5-x/esxi-5/configuring-vmware-esxi-5/

TechTarget (2014, 09 05). *techtarget*. Opgehaald van techtarget.com: http://searchnetworking.techtarget.com/tutorial/Introduction-to-firewalls-Types-of-firewalls

TechTarget (2015, 04 06). *packet-filtering*. Opgehaald van TechTarget.com: http://searchnetworking.techtarget.com/definition/packet-filtering

VMWare (2009, 04 23). *Virtualization*. Opgehaald van VMWare: https://blogs.vmware.com/virtualreality/author/eric_horschman/page/2

VMWare (2013, 07 07). *Firewall*. Opgehaald van Firewall: http://bradhedlund.com/2013/07/07/what-is-a-distributed-firewall/

VMWare (2015, 03 01). *VMware vCloud Air Network Program Product Usage Guide.* Opgehaald van VMware.com: http://v1.magibiz.net/files/admin/uploads/W285_Field_2_72903.pdf

WebOPedia (2015, 06 09). *Firewall*. Opgehaald van Webopedia.com: http://www.webopedia.com/TERM/F/firewall.html

Bijlage 1: Plan van Aanpak

Plan van Aanpak

Sentia B.V.

Vak-code: Afstuderen (TICT-AFSTUD-12)

Klas: SV3A

Versie: 0.8

Datum: 10-12-2015

R. Badal 1607426 ricky.badal@student.hu.nl

Plan van Aanpak, Utrecht, 10-12-2015

R. Badal

Versiebeheer

Hieronder volgt het versiebeheer.

Versie	Datum	Opmerkingen
0.1	16-9-2015	Origineel document opgesteld.
0.2	17-9-2015	Hoofdstukken aangepast.
0.3	17-9-2015	Hoofdvraag + deelvragen gemaakt/aangepast. Onderzoekmethoden bijgewerkt. Taal- en spelfouten gecorrigeerd.
0.4	10-11-2015	Commentaar van Roland Bijvank en Jos van Dongen verwerkt. Aanleiding bijgevoegd.
0.5	12-11-2015	Commentaar docent begeleider verwerkt. Lay-out aangepast.
0.6	13-11-2015	Commentaar Camiel en Jos verwerkt in het document en hoofd/deelvragen aangepast.
0.7	17-11-2015	Deelvraag aangepast en verdere commentaar verwerkt.
0.8	8-12-2015	Hoofdvraag aangepast en commentaar verwerkt.

TABEL 8; VERSIEBEHEER

Goedkeuring

Hieronder volgt de goedkeuringstabel.

Naam	Functie	Datum	Handtekening
C. Dobbelaar	C.T.O. Sentia		
J. van Dongen	Docent begeleider HU		
R. Badal	Afstudeerder		

TABEL 9; GOEDKEURINGSTABEL

Inhoudsopgave

Inleiding

Dit Plan van Aanpak is geschreven in opdracht voor het bedrijf Sentia. Sentia heeft voor de afstuderende student een afstudeeropdracht weten te formuleren. Deze opdracht zal voornamelijk bestaan uit het ontwerpen van een (Open Source) firewall en het geven van een advies met betrekking tot de security-eisen waaraan het ontwerp moet voldoen in combinatie met het beheer van de firewall. Dit Plan van Aanpak is tot stand gekomen uit een eerder geschreven afstudeervoorstel, geschreven door de student. Het Plan van Aanpak is geschreven voor de afstudeeropdracht; het ontwerpen van een firewall voor een virtuele omgeving. Dit Plan van Aanpak is geschreven voor de projectleider van de afstudeeropdracht, Camiel Dobbelaar, en voor de begeleidende docenten van de Hogeschool Utrecht inclusief de examencommissie.

De afstudeeropdracht is tot stand gekomen doordat in de huidige infrastructuur van Sentia het interne en externe verkeer op dezelfde firewall zitten. Mocht deze firewall dus uitvallen of aangevallen worden, dan heeft het interne en externe verkeer hier last van. Het is de taak van de student om een ontwerp te maken waar er een duidelijke scheiding is tussen het interne/externe verkeer is. De student zal een backend firewall ontwerpen voor het interne verkeer van Sentia. Dit verkeer zal dus gescheiden worden van de front-end firewall, die het externe verkeer regelt.

Dit Plan van Aanpak zal de stappen beschrijven die de student zal nemen om de opdracht zo goed mogelijk uit te voeren. Ook zal er een gedetailleerde planning worden beschreven waarin duidelijk vermeld is hoelang de opdracht zal duren en wat de op te leveren producten zullen zijn. De opdracht zal in verschillende fases verlopen, ook deze fases zullen vermeld worden in de planning.

Leeswijzer

In dit hoofdstuk vindt men een korte leeswijzer over de hoofdstukindeling en de inhoud hiervan. In het hoofdstuk ‘Beknopte Context’ wordt de organisatie beschreven en wat voor producten/diensten de organisatie aanbiedt en wat er van de student verwacht wordt. In het hoofdstuk ‘De kwestie’ wordt er duidelijk gemaakt waarom dit project gestart is en hoe de student aan de opdracht is gekomen. Ook worden de fases besproken hoe de student denk dit project aan te gaan pakken. In het hoofdstuk ‘Doelstellingen’ worden de doelstellingen die er behaald moeten worden besproken samen met de op te leveren producten. Hierna worden de hoofd en deelvragen besproken. Het theoretisch kader worden besproken in het hoofdstuk ‘Theoretisch kader’. Hierna worden de onderzoeksmethoden beschreven. De projectgrenzen worden vervolgens besproken, deze kunt u vinden in het hoofdstuk ‘Projectgrenzen’. De relatie met de studie en informatie over de stagebegeleider kunt u vinden in het volgende hoofdstuk. In het hoofdstuk ‘Planning’ bevindt zich een gedetailleerde planning over de aanpak van het project. Als laatst worden de projectrisico’s in kaart gebracht.

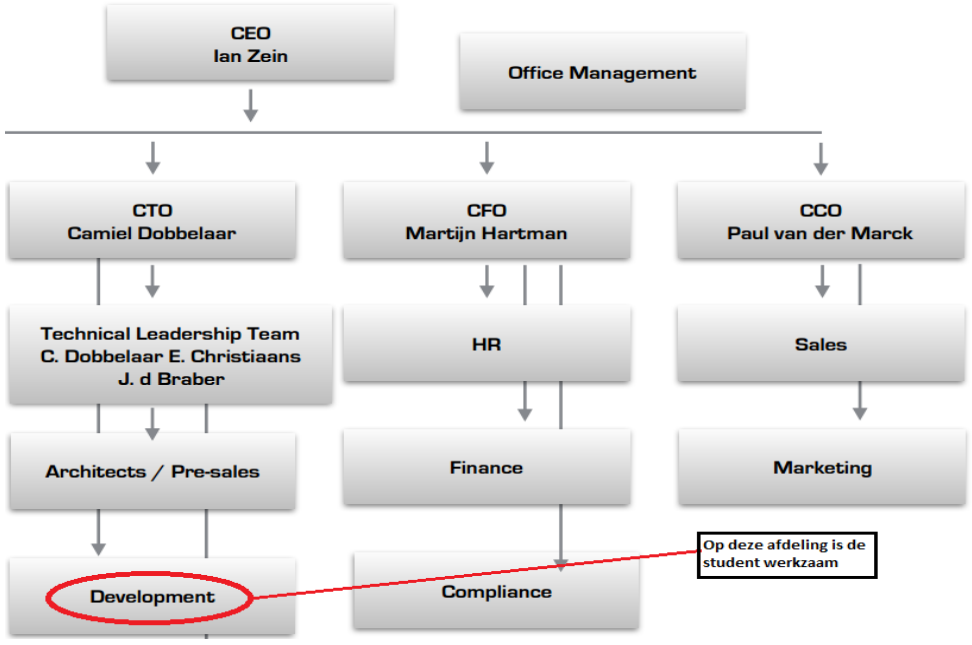
Beknopte context

Sentia B.V.

Sentia B.V. is een bedrijf dat zich specialiseert in IT-outsourcing, private en public cloud oplossingen en Technisch Applicatie Beheer. Sentia B.V. heeft een eigen private Cloud platform, genaamd; Sentia Cloud. Dit Cloud platform is speciaal ontworpen voor bedrijfs-kritische applicaties en vanuit dit platform worden er diensten aangeboden aan de klanten. Een aantal klanten van Sentia B.V. zijn onder andere; Allianz, Achmea, Unigarant, Albelli, Triodos Bank, Ennia Caribe, Amber Alert, ARAG, Univé Verzekeringen en de Consumentenbond.

Sentia B.V. telt ongeveer 70 medewerkers maar is momenteel hard aan het groeien. Het kan dus zo zijn dat wanneer de student met zijn stageperiode begint dat er een aantal medewerkers zijn bijgekomen. Binnen het bedrijf wordt er geen gebruikgemaakt van een 'vast' operating system voor de desktop Pc's. In principe zijn de medewerkers vrij in het kiezen welk operating system ze draaien. De meest voorkomende operating systems die binnen het bedrijf gebruikt worden zijn; Windows, OSx en Linux. Aan de server kant wordt er voornamelijk gebruik gemaakt van OpenBSD systemen en Windows 2012R2. Het operating system wat op de huidige firewall draait is dan ook een OpenBSD systeem.

De afdeling waar de student geplaatst zal worden is de afdeling R&D (Research & Development). Hier zal de student, samen met verschillende engineers, werken aan de verbetering/vernieuwing van het Sentia platform dat betrekking heeft op de afstudeeropdracht. Zie afbeelding 21;



AFBEELDING 21; ORGANOGRAM SENTIA

Taken/verantwoordelijkheden van de student

De voornaamste verantwoordelijkheden van de student zullen zijn om onderzoek te doen naar een software gebaseerde firewall die dient als backend firewall voor de services die Sentia B.V. levert aan haar klanten. Ook het opzetten van een beheer ontwerp, zodat het bedrijf de nieuwe firewall kan beheren, is een verantwoordelijkheid van de student. Er zal dus een ontwerp moeten worden gemaakt hoe men de nieuwe firewall kan beheren. De student heeft de bevoegdheid om gebruikt te maken van apparatuur van het bedrijf om zo een test opstellingen te kunnen maken. Op deze testopstelling kan de student onderzoek doen naar de verschillende onderwerpen. Deze bevindingen zullen gedocumenteerd worden in het onderzoeksrapport.

Het kan natuurlijk ook voorkomen dat er op kantoorhulp nodig is bij de normale werkzaamheden, echter zal de student zich voornamelijk bezig moeten houden met de afstudeeropdracht; Onderzoek doen naar een software gebaseerde backend firewall en een beheerontwerp creëren, zodat het beheer van de firewall overgedragen kan worden aan het bedrijf. Het is dus de taak van de student om een software gebaseerde backend firewall te selecteren voor het Sentia Cloud platform en een ontwerp te maken voor het beheer hiervan. De afstudeeropdracht dient zelfstandig door de student gemaakt te worden, en indien nodig met begeleiding van de bedrijfsbegeleider.

De kwestie

De opdracht die de student zal moeten uitvoeren is onderzoek doen naar een software gebaseerde firewall die als backend firewall dient voor de huidige infrastructuur. Ook dient er een beheerontwerp ontworpen te worden zodat het bedrijf het beheer na de stage van de student kan overnemen. Deze twee ontwerpen zijn gescheiden van elkaar, maar worden meegenomen in het advies dat aan Sentia zal worden geadviseerd. De opdracht is concreet te formuleren als; De student doet onderzoek naar het ontwerpen van een virtuele firewall en geeft advies hoe deze firewall het best te beheren valt. Sentia B.V. maakt momenteel gebruik van fysieke firewalls met het besturingssysteem OpenBSD. Deze fysieke firewalls dienen als 'front-end' firewalls voor de huidige infrastructuur. Omdat de infrastructuur in de afgelopen jaren flink gegroeid is, heeft Sentia B.V. als wens om een extra laag beveiliging toe te passen (de backend firewall) voor de groeiende infrastructuur. De aanleiding waar deze opdracht uit gekomen is, is dat de performance van de huidige systemen niet voldeden aan de eisen van Sentia. In de huidige situatie maakt de firewall gebruik van te veel resources om de diensten probleemloos aan te kunnen bieden aan hun klanten.

De nieuwe backend firewall zal dienen voor het interne verkeer van Sentia B.V., wat momenteel nog door de fysieke, front-end, firewalls wordt gedaan. De fysieke firewalls gebruikte te veel resources om ook nog het interne verkeer te regelen, hierdoor is de huidige situatie niet meer werkbaar. Door het implementeren van een backend firewall kunnen er dus functies worden gescheiden. Zo zullen de fysieke firewalls verantwoordelijk zijn voor het verkeer van en naar het internet, en zal de backend firewall verantwoordelijk zijn voor het interne verkeer binnen het bedrijf. Bij een DDoS-aanval op de externe (front-end) firewall, zal de externe (backend) firewall dus gewoon blijven functioneren en kan er intern nog doorgewerkt worden. Zo kunnen de verschillende functies worden gescheiden bij de implementatie. Bij het onderzoeken/ implementeren van de backend firewall moet er rekening gehouden worden met een aantal factoren, namelijk:

- Kosten (voorkeur heeft Open Source, een betaald alternatief mag ook mits dit binnen het bedrijf past qua infrastructuur en eisen/wensen)
- Performance (De firewall moet onder hoge verkeersdrukte optimaal kunnen presteren)
- Redundantie/high availability (mocht er een instantie van de firewall uitvallen, dan dient er een back-up firewall geactiveerd te worden en de taken over te nemen)
- Integratie met VMWare (de firewall dient implementeerbaar te zijn in de huidige omgeving)
- Routeringsprotocollen (ospf, etc.)
- Andere protocollen (802.1q, vxlan)
- Beheerbaarheid (de firewall dient vanuit een centrale plek beheerbaar te zijn)
- Ontwikkelingsuren (om het bruikbaar te krijgen)

Omdat de huidige front-end firewalls op het Open Source systeem OpenBSD draaien en Sentia B.V. zo flexibel mogelijk wilt blijven, heeft een Open Source firewall de voorkeur. Een commercieel alternatief ter ijking van de functionaliteit is wenselijk om de vergelijking tussen een commercieel en gratis variant te vergelijken. Om de opdracht zo gestructureerd mogelijk aan te pakken, worden er een aantal fases doorlopen, namelijk;

- Onderzoeksfase
- Ontwerpfase
- Validatie (besluitvorming over het advies)
- Implementatie fase
- Documentatie fase

Onderzoek fase

Tijdens deze fase zal er onderzoek gedaan worden naar verschillende (Open Source) firewalls. De verschillende pakketten zullen met elkaar vergeleken worden en aan het eind van deze fase zal er een keuze worden gemaakt voor het beste pakket. Ook zal er onderzocht worden hoe de pakketten te beheren zijn en zal er een beheerplan worden ontworpen voor het gekozen pakket. Het doel van deze fase is dus om onderzoek te doen naar een pakket dat alle eisen voldoet en het onderzoeken van het beheer van het gekozen pakket.

Ontwerpfase

Tijdens deze fase zal er een ontwerp worden gemaakt met het gekozen pakket. Er zal worden gekeken waar de firewall het best geplaatst kan worden. Dit zal in overeenstemming met de begeleidende bedrijfsleider worden gedaan. Het doel van deze fase is dus om een ontwerp te maken van de infrastructuur met de implementatie van de nieuwe backend firewall. Ook zal er een ontwerp worden ontworpen voor het beheer. Het doel van dit beheerontwerp is om het beheer over te dragen aan het bedrijf nadat de student klaar is met zijn stage.

Validatie fase

Tijdens deze fase zal er gekeken worden naar het gekozen pakket en het beheerontwerp. Er zal samen met de bedrijfsbegeleider worden gekeken of het pakket en het ontwerp voldoen aan de eisen die Sentia B.V. verwacht van de nieuwe backend firewall. Indien Sentia B.V. akkoord is met de gemaakte keuzes kan er door worden gegaan naar de volgende fase, de ontwerp fase. Indien het bedrijf niet akkoord is met de gemaakte keuzes dan zal er terug worden gegaan naar de onderzoeksfase. Het doel van de validatie fase is dus om samen met Sentia en de student te kijken of de wensen, eisen en gemaakte keuzes goed verwerkt zijn en, indien akkoord, door te gaan naar de ontwerpfase.

Implementatie fase

In deze fase zal het Proof of Concept worden gebouwd. Dit houdt dus in dat de student een Proof of Concept zal maken met het gekozen pakket en ontwerp en het pakket, samen met het ontwerp, zal aantonen aan de stage/bedrijfsbegeleider. Tijdens het Proof of Concept moet de student kunnen aantonen dat alle wensen en eisen van Sentia B.V. zijn meegenomen in het Proof of Concept en de student dient dit werkend aan te tonen aan de betreffende begeleiders. Dit kan gedaan worden door middel van een testplan. In het testplan staan alle functies die moeten werken en moeten voldoen aan de wensen van de klant.

Het doel van deze fase is dus om het Proof of Concept werkend te laten zien met inachtneming van de eisen die Sentia B.V. stelt aan het gekozen pakket.

Documentatie fase

Tijdens deze fase zullen de bevindingen worden gedocumenteerd. De bevindingen per fases zullen ook worden gedocumenteerd, deze bevindingen zullen als bijlage dienen in het uiteindelijke document dat opgeleverd zal worden. De bevindingen die opgedaan en gedocumenteerd zijn in de onderzoeksfase kunnen als handleiding gebruikt worden voor het installeren/configureren van eventuele software. Het beheer van het pakket in de onderzoeksfase zal ook worden gedocumenteerd in het onderzoeksrapport. Het uiteindelijke beheerontwerp zal als bijlage dienen in het onderzoeksrapport. Het doel van deze fase is dat een medewerker van Sentia B.V. de nieuwe infrastructuur kan opbouwen op basis van de documentatie van de student.

Doelstelling

De doelstelling van de afstudeeropdracht voor de student is om een advies te geven, na de onderzoeksfase, met betrekking tot het ontwerpen van een (open source) firewall. Ook dient er advies gegeven te worden over het beheren van de firewall en dient deze gedocumenteerd te worden in een beheerplan. De resultaten van het onderzoek naar het product (de backend firewall) zullen gedocumenteerd worden en er zal een Proof of Concept worden gebouwd om de functies van de firewall werkend aan het bedrijf te laten zien. Dit zal worden aangetoond aan het einde van de afstudeerstage, maart/april 2016.

Type opdracht

De opdracht die de student zal moeten uitvoeren is een ontwerp/onderzoeksopdracht. Dit omdat er onderzoek gedaan zal worden naar het product (de backend firewall) en er een ontwerp zal worden ontworpen voor de firewall en om het beheer over te dragen aan het bedrijf. In dit ontwerp zal er duidelijk worden gemaakt hoe het bedrijf de nieuwe firewall kan beheren en op welke aspecten het bedrijf moet letten tijdens het beheer.

Op te leveren producten

De volgende producten dienen tijdens het afstuderen worden opgeleverd;

- Plan van Aanpak
- Onderzoeksrapport (met advies)
- Functioneel Ontwerp (met beheerplan)
- Technisch Ontwerp
- Test plan
- Proof of Concept
- Scriptie/advies

Al deze producten dienen met een voldoende worden afgerond ter afronding van de afstudeerdopdracht.

Kwaliteitsborging

Om de kwaliteit van de op te leveren producten zo hoog mogelijk te houden zijn er afspraken gemaakt met Sentia. De afspraken zijn als volgt;

- De voortgang zal wekelijks besproken worden met de opdrachtgever.
- Feedback voor de op te leveren producten zal binnen een week worden verwerkt door de student.
- De op te leveren documenten zullen nagekeken worden op taal en spelfouten.
- Technische documentatie zal door technici worden nagekeken.
- Er zullen interviews plaatsvinden om onduidelijkheden te voorkomen.

Hoofdvraag

De hoofdvraag is als volgt geformuleerd: *"Welk type firewall voldoet het meest aan de gestelde eisen van het bedrijf en is het meest geschikt voor de huidige infrastructuur?"*

Deelvragen

De deelvragen zijn als volgt geformuleerd;

- Welke verschillen zijn er tussen een open source (gratis) firewall en een closed souce (betaalde) firewall?
- Welke firewall functies dienen er beschikbaar te zijn om aan de eisen van de klant te voldoen?
- Welke risico's zijn er bij het implementeren van een firewall in een bestaande omgeving?
- Op welke manier wordt de firewall gemonitord?
- Wat zijn de voor en nadelen van een virtuele firewall ten opzichte van een fysieke firewall?

Theoretisch Kader

Om goed onderzoek te kunnen doen naar de verschillende onderwerpen zal er gekeken moeten worden welke technieken en methoden er gebruikt worden binnen Sentia B.V. Ook zal er gekeken worden naar verschillende methodieken en technieken die toegepast worden bij andere bedrijven om zo een vergelijking te maken en te kijken wat de beste manier van aanpak is. Omdat de opdracht voornamelijk bestaat uit onderzoek doen naar een backend firewall in een huidige groeiende infrastructuur en een ontwerp creëren voor het in beheer nemen van de firewall, zijn er wel een aantal onderwerpen waar de student vast onderzoek naar kan doen, namelijk:

- Firewall
- Open Source
- Linux
- Performance
- High availability
- Routering
- iTiL
- Beheerplan
- IPS
- VLAN's
- 802.1q
- Veiligheid/Security

Als de student zich verdiept heeft in deze onderwerpen kan er met het bedrijf worden afgestemd of de gevonden resultaten betrekking hebben met de eisen en wensen van het product. De resultaten van het onderzoek naar de bovengenoemde onderwerpen zullen in het onderzoeksrapport worden beschreven en aan het eind van het onderzoeksrapport zal er een advies worden gegeven welk pakket/software er het best in de infrastructuur past binnen het bedrijf.

Onderzoeksmethoden

Om zo goed mogelijk antwoord te kunnen geven op de hoofdvraag en deelvragen zullen er verschillende onderzoeksmethoden/technieken gebruikt worden tijdens het afstuderen door de student. Deze technieken zullen helpen bij het beantwoorden van de vragen. Hieronder in tabel 10 vindt u een overzicht van de methoden die er gebruikt kunnen worden tijdens de afstudeeropdracht;

TABEL 10; ONDERZOEKSMETHODEN

Vragen	Methoden	Opmerkingen
Welke verschillen zijn er tussen een open source (gratis) firewall en een closed souce (betaalde) firewall?	Research	Met het gebruik van deze methode kan de student erachter komen welke functies er beschikbaar zijn bij een betaalde firewall en of dezelfde functies ook beschikbaar zijn bij een open source alternatief.
Welke firewall functies dienen er beschikbaar te zijn om aan de eisen van de klant te voldoen?	Interview	Door interviews te doen kan de student deze deelvraag beantwoorden.

Welke risico's zijn er bij het implementeren van een firewall in een bestaande omgeving?	Research	Tijdens de onderzoeksfase zal er een test omgeving worden opgezet. In deze omgeving kan de student achter de risico's komen van het implementeren van een firewall in een bestaande omgeving.
Hoe wordt de firewall gemonitord?	Interview	D.m.v. interviews kan de student erachter komen hoe bepaalde services gemonitord worden binnen het bedrijf. Ook kan de student voorstellen om de firewall mee te nemen in de huidige monitoring.
Wat zijn de voor en nadelen van een virtuele firewall ten opzichte van een fysieke firewall?	Research/testen in een testomgeving	D.m.v. het testen van bepaalde opstellingen kan de student erachter komen wat de voor/nadelen zijn van een virtuele/fysieke firewall.

TABEL 11; ONDERZOEKSMETHODEN

Projectgrenzen

Tijdens het onderzoek heeft de student een aantal verantwoordelijkheden. De student is verantwoordelijk voor de volgende taken;

- Het opstellen van een Plan van Aanpak
- Onderzoek doen naar de wensen/eisen van de klant.
- Het maken van een firewall ontwerp.
- Het maken van een beheer ontwerp.
- Advies geven omtrent de bovenstaande onderwerpen.
- Het aantonen van een werkende situatie (PoC).
- Het opstellen van een test plan.
- Het schrijven van een afstudeerscriptie (advies) voor het bedrijf

De onderstaande taken vallen niet onder de verantwoordelijkheid van de student;

- Het verrichten van 'normale' werkzaamheden.
- Het beheer van de externe (front-end) firewall.
- Het maken van een implementatieplan.

Relatie met studie

De studie die de student volgt is de studie System and Network Engineering. De opdracht heeft een goede relatie met de studie. Dit omdat er tijdens de studie soort gelijken project zijn uitgevoerd tijdens de themaopdracht. De projecten tijdens de themaopdracht verschillen wel met de afstuuropdracht, omdat het bedrijf andere eisen en wensen heeft dan de opdrachtgever tijdens de projecten. Het doel van de opdracht is om een (open source) backend firewall te implementeren in een huidige, groeiende infrastructuur. Hierbij komen veel zaken kijken die de student heeft geleerd tijdens zijn studie, onder andere; het inrichten van een netwerk, een firewall inrichten, OS inrichten, routering, security en scripting.

Onderbouwing Bedrijfsbegeleider

Tijdens mijn afstudeerstage zal ik begeleid worden door Camiel Dobbelaar. Camiel Dobbelaar is CTO (Chief Technology Officer) bij Sentia B.V.. Tijdens mijn gesprek met Camiel is het gebleken dat Camiel over een zeer grote technische kennis bezit. Camiel heeft zijn opleiding gevolgd bij de Universiteit Twente. Hierdoor is Camiel in staat om de student om een minimaal hbo-niveau te kunnen begeleiden. Voor zijn baan bij Sentia B.V. heeft Camiel bij TomTom, XS4ALL, Shell en KPN gewerkt. Bij deze bedrijven heeft Camiel altijd een technische functie gehad. Door al deze technische ervaringen kan Camiel de student goed begeleiden met technische problemen.

Beschrijving betrokkenen

Tijdens het afstuderen kan het zijn dat bepaalde taken worden overgenomen van de heer Dobbelaar om de student te begeleiden. Dit zal hoogstwaarschijnlijk een netwerk engineer zijn. Wie dit precies is, is nog niet duidelijk. Indien er in een ander stadium meer duidelijkheid verschaft zal worden hierover, zal dit door de student worden gedocumenteerd.

Bedrijfs-/Persoonsgegevens

Sentia B.V.
Vestiging Amsterdam:

MediArena 7
1114 BC Amsterdam
088 - 4242 200

Vestiging Nieuwegein (afstudeerdersplek):

Einsteinbaan 4
3439 NJ Nieuwegein
088 - 4242 200

Bedrijfsbegeleider:

Naam:	Camiel Dobbelaar
E-mail:	camiel.dobbelaar@sentia.com
Linkdin:	https://nl.linkedin.com/pub/camiel-dobbelaar/0/146/9aa
Telefoon:	088 – 4242 200

Docentbegeleider HU:

Naam:	Jos van Dongen
E-mail:	jos.vandongen@hu.nl
Telefoon:	06 - 24213447

Planning

De afstudeeropdracht duurt ongeveer 17 weken en zal waarschijnlijk op 10 november beginnen. Op basis van deze tijdsperiode (840 uur) is er een globale planning gemaakt. De planning kunt u vinden in tabel 12 hieronder;

TABEL 12; PLANNING

Datum	Werkzaamheden	Aantal uur
10-11-2015 t/m 30-11-2015 (3 weken)	• Beginnen bij het bedrijf. • Gesprekken met bedrijfsbegeleiders • Eerste versie PvA opstellen Op de leveren producten: Eerste versie van het Plan van Aanpak	100 uur 10 uur 40 uur **Totaal: 150**
01-12-2105 t/m 23-12-2015 (4 weken)	• Afstudeer contract opstellen • Plan van Aanpak afronden • Onderzoek doen naar het op te leveren product • Eerste versie onderzoeksrapport opstellen • Gesprekken met bedrijfsbegeleiders • Beginnen met het Functioneel Ontwerp Op te leveren producten: Definitieve versie van het Plan van Aanpak. Eerste opzet onderzoeksrapport met advies. Eerste opzet van het Functioneel Ontwerp met beheerplan.	10 uur 10 uur 60 uur 50 uur 10 uur 70 uur **Totaal**: **210**
28-12-2015 t/m 22-01-2016 (4 weken)	• Definitieve versie onderzoeksrapport • Eerste opzet Technisch Ontwerp • Gesprekken met bedrijfsbegeleiders • Functioneel Ontwerp afronden • Technisch Ontwerp afronden • Test plan opstellen • Gesprekken met bedrijfsbegeleiders • Test plan afronden • Proof of Concept voorbereiden • Proof of Concept bouwen • Gesprekken met bedrijfsbegeleiders • Proof of Concept documenten	30 uur 70 uur 10 uur 20 uur 20 uur 10 uur 10 uur 30 uur 50 uur 10 uur 20 uur

	<u>Op te leveren producten:</u> Onderzoeksrapport, Functioneel Ontwerp, Technisch Ontwerp en een testplan.	**Totaal: 160**
25-01-2016 t/m 22-03-2106 (12 weken)	• Eerste opzet scriptie • Gesprekken met bedrijfsbegeleiders • Scriptie afronden <u>Op te leveren producten:</u> Definitieve versie scriptie.	120 uur 10 uur 160 uur **Totaal: 290**
29-03-2016	• Presentatie voorbereiden • Presentatie presenteren <u>Op te leveren producten:</u> Presentatie.	29 uur 1 uur **Totaal: 30**

Risico’s

Aan elk project dat er uitgevoerd wordt zitten natuurlijk risico’s. Om de risico’s zo goed mogelijk proberen te vermeiden is er een globale planning gemaakt, zie hoofdstuk ‘Globale Planning’. Ook bij dit project kunnen er zich een aantal risico’s voordoen. Hieronder, in tabel 13, ziet u een aantal risico’s die zich kunnen voordoen tijdens dit project:

TABEL 13; RISICO'S

Risico	Maatregel
Ontwerp past niet in de huidige infrastructuur	• Ontwerp aanpassen • Beheerplan wijzigen en de juiste eisen hierin verwerken.
Onduidelijkheid over het beheer	• Beheerplan aanpassen en duidelijk maken hoe het beheer moet worden gedaan.
Tijd te kort bij een eindproduct	• Extra uren inplannen en eventueel deadline proberen uit te stellen.
Benodigde resources zijn niet beschikbaar	• Planning aanpassen en bekijken hoelang het duurt voordat de resources beschikbaar zijn. • Alternatief zoeken om de resources ergens anders vandaan te halen.
Product voldoet niet aan de eisen van de klant	• Alternatieven zoeken voor het product. • Gesprek met begeleiders en eisen goed in kaart brengen. • Kans op uitloop van de stage, dus extra tijd aanvragen.

Bibliografie

B.V., S. (sd). *Sentia B.V*. Opgeroepen op juni 2015, van Sentia B.V: https://www.sentia.com/

Dobbelaar, C. (2015, Juni 11). CTO. (R. Badal, Interviewer)

Steenhouder, M. (sd). *Leren Communiceren.* Wolters Noordhof.

Bijlage 1; contract afstudeeropdracht

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

Datum:	_____
Naam student:	Ricky Badal
Opleiding:	Systeembeheer
Variant:	Voltijd
Adres student:	Vasteland 381
Postcode/woonplaats student:	3011BJ, Rotterdam
Studentnummer:	1607426
Telefoonnummer privé:	0655126066
E-mailadres:	ricky.badal@student.hu.nl
Naam bedrijf (afstuderen):	Sentia B.V.
Adres bedrijf:	Einsteinbaan 4
Postcode/woonplaats bedrijf:	3439NJ, Nieuwegein
Naam bedrijfsbegeleider:	C. Dobbelaar
Telefoonnummer bedrijfsbegeleider:	088 002 2700
E-mailadres bedrijfsbegeleider:	camiel.dobbelaar@sentia.com
Beoogde datum van afstuderen:	_____

Geheimhouding geaccordeerd door HU op: _____

Ondergetekenden verklaren akkoord te gaan met de inhoud van aangehecht plan van aanpak.

Handtekeningen

Student: _____

Docentbegeleider: _____

Bedrijfsbegeleider: _____

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

Bijlage 2: Afstudeervoorstel

Projectvoorstel

Sentia B.V.

Vak-code: Afstuderen (TICT-AFSTUD-12)

Klas: SV3A

Versie: 1.0

Datum: 6-7-2015

R. Badal 1607426 ricky.badal@student.hu.nl

Projectvoorstel, Utrecht, 6-7-2015

R. Badal

Versiebeheer

Hieronder in volgt het versiebeheer.

Versie	Datum	Opmerkingen
0.1	26-5-2015	Origineel document opgesteld
0.2	20-6-2015	Eerste 'draft' van het document gemaakt.
0.3	6-7-2015	1ste comments van Harry Beerlage verwerkt.
0.4	7-7-2015	Opdracht aangepast en het beheer erbij betrokken.
0.5	7-8-2015	Doelstellingen aangepast

TABEL 7

Inhoudsopgave

Inleiding

In dit document zal het projectvoorstel van het bedrijf Sentia B.V. worden beschreven. Tijdens het afstuderen is het aan de studenten om een stage plek te zoeken waar de studenten kunnen afstuderen. Omdat dit het laatste traject is van de HBO opleiding, dient deze stage plek wel aan een aantal eisen te voldoen. De eisen staan beschreven in de afstudeerleidraad. Tijdens mijn zoektocht naar een stage plek ben ik bij het bedrijf Sentia B.V. gekomen. Dit document is gebaseerd op het afstudeerleidraad, paragraaf 7.1.

Context

Sentia B.V.

Sentia B.V. is een bedrijf dat zich specialiseert in IT outsourcing, private en public Cloud oplossingen en Technisch Applicatie Beheer. Sentia B.V. heeft een eigen private Cloud platform, genaamd; Sentia Cloud. Dit Cloud platform is speciaal ontworpen voor bedrijf kritische applicaties en vanuit dit platform worden er diensten aangeboden aan de klanten. Een aantal klanten van Sentia B.V. zijn onder andere; Allianz, Achmea, Unigarant, Albelli, Triodos Bank, Ennia Caribe, Amber Alert, ARAG, Univé Verzekeringen en de Consumentenbond.

Sentia B.V. telt ongeveer 70 medewerkers maar is momenteel hard aan het groeien. Het kan dus zo zijn dat wanneer mijn stage periode begint dat er een aantal medewerkers zijn bijgekomen. Binnen het bedrijf wordt er geen gebruik gemaakt van een 'vast' operating system voor de desktop Pc's. In principe zijn de medewerkers vrij in het kiezen welk operating system ze draaien. De meest voorkomende operating systems die binnen het bedrijf gebruikt worden zijn; Windows, OSx en Linux. Aan de server kant wordt er voornamelijk gebruik gemaakt van OpenBSD systemen en Windows 2012R2. Het operating system wat op de huidige firewall draait is dan ook een OpenBSD systeem.

De afdeling waar de student geplaatst zal worden is de afdeling R&D (Research & Development). Hier zal de student, samen met verschillende engineers, werken aan de verbetering/vernieuwing van het Sentia platform dat betrekking heeft met de afstudeeropdracht.

Taken / verantwoordelijkheden van de student

De voornaamste verantwoordelijkheden van de student zullen zijn om onderzoek te doen naar een software gebaseerde firewall die dient als backend firewall voor de services die Sentia B.V. levert aan haar klanten. Ook het opzetten van een beheer ontwerp (volgens de ITIL methoden), zodat het bedrijf de nieuwe firewall kan beheren is een verantwoordelijkheid van de student. Er zal dus een ontwerp moeten worden ontworpen hoe men de nieuwe firewall kan beheren. Het kan natuurlijk ook voorkomen dat er op kantoor hulp nodig is bij de normale werkzaamheden, echter zal de student zich voornamelijk bezig moeten houden met de afstudeeropdracht; Onderzoek doen naar een software gebaseerde backend firewall en een beheerontwerp creëren zodat het beheer van de firewall overgedragen kan worden aan het bedrijf. Het is dus de taak van de student om een software gebaseerde backend firewall te selecteren voor het Sentia Cloud platform en een ontwerp te maken voor het beheer hiervan. De afstudeeropdracht dient zelfstandig door de student gemaakt te worden, en indien nodig met begeleiding van de bedrijfsbegeleider.

Relatie met andere projecten

Tot zo ver bekend heeft dit afstudeerproject geen relatie met andere projecten.

Opdrachtformulering

De opdracht die de student zal moeten uitvoeren is onderzoek doen naar een software gebaseerde firewall die als backend firewall dient voor de huidige infrastructuur. Ook dient er een beheerontwerp ontworpen te worden volgens die ITIL methoden zodat het bedrijf het beheer na de stage van de student kan overnemen. Sentia B.V. maakt momenteel gebruik van fysieke firewalls met het besturingssysteem OpenBSD. Deze fysieke firewalls dienen als 'front-end' firewalls voor de huidige infrastructuur. Omdat de infrastructuur in de afgelopen jaren flink gegroeid is, heeft Sentia B.V. als wens om een extra laag beveiliging toe te passen (de backend firewall) voor de groeiende infrastructuur. Deze backend firewall zal dienen voor het interne verkeer van Sentia B.V., wat momenteel nog door de fysieke, front-end, firewalls wordt gedaan. Door het implementeren van een backend firewall kunnen er dus functies worden gescheiden. Zo zullen de fysieke firewalls verantwoordelijk zijn voor het verkeer van en naar het internet, en zal de backend firewall verantwoordelijk zijn voor het interne verkeer binnen het bedrijf. Bij een DDoS aanval op de externe (front-end) firewall, zal de externe (backend) firewall dus gewoon blijven functioneren en kan er intern nog doorgewerkt worden. Zo kunnen de verschillende functies worden gescheiden bij de implementatie. Bij het onderzoeken / implementeren van de backend firewall moet er rekening gehouden worden met een aantal factoren, namelijk:

- Kosten
- Performance
- Redundantie / high availability
- Integratie met VMWare
- Routeringsprotocollen (ospf, etc.)
- Andere protocollen (802.1q, vxlan)
- Beheerbaarheid
- Ontwikkelingsuren (om het bruikbaar te krijgen)

Omdat de huidige front-end firewalls op het Open Source systeem OpenBSD draaien en Sentia B.V. zo flexibel mogelijk wilt blijven, heeft een Open Source firewall de voorkeur. Een commercieel alternatief ter ijking van de functionaliteit is wenselijk om de vergelijking tussen een commercieel en gratis variant te vergelijken. Om de opdracht zo gestructureerd mogelijk aan te pakken, worden er een aantal fases doorlopen, namelijk;

- Onderzoek fase
- Ontwerp fase
- Validatie fase
- Implementatie fase
- Documentatie fase

Onderzoek fase
Tijdens deze fase zal er onderzoek gedaan worden naar verschillende (Open Source) firewalls. Hierbij zal rekening gehouden worden met de factoren die vermeld zijn in het hoofdstuk *Opdrachtformulering*. De verschillende pakketten zullen met elkaar vergeleken worden en aan eind van deze fase zal er een keuze worden gemaakt voor het beste pakket. Het doel van deze fase is dus om onderzoek te doen naar een pakket die aan alle eisen voldoet.

Ontwerp fase
Tijdens deze fase zal er een ontwerp worden gemaakt met het gekozen pakket. Er zal worden gekeken waar de firewall het best geplaatst kan worden. Dit zal in overeenstemming met de begeleidende bedrijfsleider worden gedaan. Het doel van deze fase is dus om een ontwerp te maken van de infrastructuur met de implementatie van de nieuwe backend firewall. Ook zal er een ontwerp worden ontworpen voor het beheer. Dit ontwerp zal volgens de ITIL methoden worden ontworpen. Het doel van dit beheerontwerp is om het beheer over te dragen aan het bedrijf nadat de student klaar is met zijn stage.

Validatie fase
Tijdens deze fase zal er gekeken worden naar het gekozen pakket en het nieuwe beheerontwerp. Er zal samen met de bedrijfsbegeleider worden gekeken of het pakket en het ontwerp voldoen aan de eisen die Sentia B.V. verwacht van de nieuwe backend firewall. Indien Sentia B.V. akkoord is met de gemaakte keuzes kan er door worden gegaan naar de volgende fase, Implementatie. Het doel van de validatie fase is dus om samen met Sentia en de student te kijken of de wensen, eisen en gemaakte keuzes goed verwerkt zijn en, indien akkoord, door te gaan naar de implementatie fase.

Implementatie fase
In deze fase zal het Proof of Concept worden gebouwd. Dit houdt dus in dat de student een Proof of Concept zal maken met het gekozen pakket en ontwerp en dit zal aantonen aan de stage / bedrijfsbegeleider. Tijdens het Proof of Concept moet de student kunnen aantonen dat alle wensen en eisen van Sentia B.V. zijn meegenomen in het Proof of Concept en de student dient dit werkend aan te tonen aan de betreffende begeleiders. Het doel van deze fase is dus om het Proof of Concept werkend te laten zien met in acht neming van de eisen die Sentia B.V. stelt aan het gekozen pakket.

Documentatie fase
Tijdens deze fase zullen de bevinden worden gedocumenteerd. De bevindingen per fases zullen ook worden gedocumenteerd, deze bevindingen zullen als bijlage dienen in het uiteindelijke document dat opgeleverd zal worden. Het doel van deze fase is dat een medewerker van Sentia B.V. de nieuwe infrastructuur kan opbouwen op basis van de documentatie van de student.

De kwestie

De opdracht is tot stand gekomen door de groeiende infrastructuur van Sentia B.V.. Doordat de infrastructuur blijft groeien is er behoefte aan een backend firewall die de infrastructuur beheerbaar en veilig houdt in de toekomst. Ook zal er een ontwerp worden gedaan voor het beheer, om zo het beheer over te kunnen dragen aan het bedrijf. Onderwerpen die bij dit project horen zijn onder andere;

- Veiligheid / Security
- Open Source
- Linux
- ITIL
- Performance
- High availability
- Routering
- IPS
- VLAN's
- 802.1q
- Beheer
- Beheerplan
- Gegevensbeheer
- Performancebeheer

Doelstelling

De doelstelling van de afstudeeropdracht voor de student is om een beheerontwerp te creëren dat het mogelijk maakt om het product, waar onderzoek naar gedaan is, te beheren en dit op een zo duidelijk mogelijke wijze gedocumenteerd te hebben zodat het beheer van het product overgedragen kan worden aan het bedrijf. De resultaten van het onderzoek naar het product (de backend firewall) zullen gedocumenteerd worden en er zal een Proof of Concept worden gebouwd om de functies van de firewall werkend aan het bedrijf te laten zien.

Soort Opdracht

De opdracht die de student zal moeten uitvoeren is een ontwerp/onderzoeksopdracht. Dit omdat er onderzoek gedaan zal worden naar het product (de backend firewall) en er een ontwerp zal worden ontworpen om het beheer over te dragen aan het bedrijf. In dit ontwerp zal er duidelijk worden gemaakt hoe het bedrijf de nieuwe firewall kan beheren en op welke aspecten het bedrijf moet letten tijdens het beheer.

Op te leveren producten

De volgende producten dienen tijdens het afstuderen worden opgeleverd;

- Plan van Aanpak
- Functioneel Ontwerp
- Beheerplan
- Technisch Ontwerp
- Test plan
- Proof of Concept
- Scriptie

Al deze producten dienen met een voldoende worden afgerond ter afronding van de afstudeerdopdracht.

Globale aanpak

Om de opdracht zo goed mogelijk uit te kunnen voeren zal de student eerst naar de gebruikte methoden en technieken binnen het bedrijf moeten kijken. Er zullen verschillende interviews plaats vinden met het bedrijf om zo de eisen en wensen goed in kaart te brengen. Hierbij hoort ook de literatuuronderzoek voor de verschillende onderwerpen. Door middel van de interviews en de daaruit komende informatie kan er gekeken worden wat er allemaal in het Functioneel Ontwerp dient te komen. In het Functioneel Ontwerp staan de functies beschreven waaraan de backend firewall moet voldoen. Als deze informatie eenmaal verwerkt is kan de eerste versie van het Functioneel Ontwerp worden opgesteld. Hierna zal er gekeken moeten worden wat er in

het Technisch Ontwerp zal moeten komen. De technische specificaties van de functionaliteiten zullen hierin beschreven worden. Nadat alle partijen akkoord zijn met het Functioneel en Technisch Ontwerp zal er een Proof of Concept en een test plan worden opgesteld om te kijken of het opgeleverde product daadwerkelijk aan de eisen en wensen van de klant voldoet. Alle bevindingen die de student doet zullen gedocumenteerd worden. Door deze manier van aanpak is het mogelijk dat het opgeleverde product nagebouwd kan worden door een andere partij.

Hoofdvraag

Hoe kan het security beleid van Sentia B.V. concreet verbeterd worden, door rekening te houden met verschillende functies die door verschillende security componenten voldaan moeten worden?

Theoretisch Kader

Om goed onderzoek te kunnen doen naar de verschillende onderwerpen zal er gekeken moeten worden welke technieken en methoden er gebruikt worden binnen Sentia B.V.. Omdat de opdracht voornamelijk bestaat uit onderzoek doen naar een backend firewall in een huidige groeiende infrastructuur en een ontwerp creëren voor het in beheer nemen van de firewall, zijn er wel een aantal onderwerpen waar de student vast onderzoek naar kan doen, namelijk:

- Firewall
- Open Source
- Linux
- Performance
- High availability
- Routering
- iTiL
- Beheerplan
- IPS
- VLAN’s
- 802.1q

Als de student zich verdiept heeft in deze onderwerpen kan er met het bedrijf worden afgestemd of de gevonden resultaten betrekking hebben met de eisen en wensen van het product. De resultaten van het onderzoek naar de bovengenoemde onderwerpen zullen in het Functioneel Ontwerp worden beschreven.

Trefwoorden / Begrippen

Hieronder bevindt zich een lijst met een aantal trefwoorden waarmee de opdracht wordt gekarakteriseerd:

- VMWare
- Statefull Firewall
- OpenBSD
- FreeBSD
- OpenSource
- iTiL
- Beheerplan
- Linux
- pfSense
- Projectdocumentatie
- High Availability
- Routering
- SDN
- IPS
- OSPF
- IPtables
- IPfw

Relatie met studie

De studie die de student volgt is de studie System and Network Engineering. De opdracht heeft een goede relatie met de studie. Dit omdat er tijdens de studie soort gelijken project zijn uitgevoerd tijdens de themaopdracht. De projecten tijdens de themaopdracht verschillen wel met de afstuuropdracht, omdat het bedrijf andere eisen en wensen heeft dan de opdrachtgever tijdens de projecten. Het doel van de opdracht is om een (open source) backend firewall te implementeren in een huidige, groeiende infrastructuur. Hierbij komen veel zaken kijken die de student heeft geleerd tijdens zijn studie, onder andere; het inrichten van een netwerk, een firewall inrichten, OS inrichten, routering, security en scripting.

Onderbouwing Bedrijfsbegeleider

Tijdens mijn afstudeerstage zal ik hoogstwaarschijnlijk door Camiel Dobbelaar worden begeleidt. Camiel Dobbelaar is CTO (Chief Technology Officer) bij Sentia B.V.. Tijdens mijn gesprek met Camiel is het gebleken dat Camiel over een zeer grote technische kennis bezit. Camiel heeft zijn opleiding gevolgd bij de Universiteit Twente. Hierdoor is Camiel in staat om de student om een minimaal HBO niveau te kunnen begeleiden. Voor zijn baan bij Sentia B.V. heeft Camiel bij TomTom, XS4ALL, Shell en KPN gewerkt. Bij deze bedrijven heeft Camiel altijd een technische functie gehad. Door al deze technische ervaringen kan Camiel de student goed begeleiden met technische problemen.

Beschrijving Betrokkenen

Tijdens het afstuderen kan het zijn dat bepaalde taken worden overgenomen van de heer Dobbelaar om de student te begeleiden. Dit zal hoogstwaarschijnlijk een netwerk engineer zijn. Wie dit precies is, is nog niet duidelijk. Indien er in een ander stadium meer duidelijkheid verschaft zal worden hierover, zal dit door de student worden gedocumenteerd.

Bedrijfs-/Persoonsgegevens

Sentia B.V.
Vestiging Amsterdam:

MediArena 7
1114 BC Amsterdam
088 - 4242 200

Vestiging Nieuwegein:

Einsteinbaan 4
3439 NJ Nieuwegein
088 - 4242 200

Bedrijfsbegeleider:

Camiel Dobbelaar
camiel.dobbelaar@sentia.com
https://nl.linkedin.com/pub/camiel-dobbelaar/0/146/9aa

Planning

De afstudeeropdracht duurt ongeveer 17 weken en zal waarschijnlijk op 31 augustus beginnen. Op basis van deze tijdsperiode (840 uur) is er een globale planning gemaakt. De planning kunt u vinden in tabel 14 hieronder;

TABEL 14; GLOBALE PLANNING

Datum	Werkzaamheden	Aantal uur
02-11-2015 t/m 30-11-2015 (5 weken)	• Beginnen bij het bedrijf. • Gesprekken met bedrijfsbegeleiders • Eerste versie PvA opstellen	70 uur 10 uur 40 uur **Totaal: 120**
01-12-2105 t/m 23-12-2015 (4 weken)	• Afstudeer contract opstellen • Plan van Aanpak afronden • Onderzoek doen naar het op te leveren product • Gesprekken met bedrijfsbegeleiders • Beginnen met het Functioneel Ontwerp	10 uur 10 uur 170 uur 10 uur 70 uur **Totaal**: **270**
28-12-2015 t/m 22-01-2016 (4 weken)	• Eerste opzet Technisch Ontwerp • Gesprekken met bedrijfsbegeleiders • Technisch Ontwerp afronden • Test plan opstellen • Gesprekken met bedrijfsbegeleiders • Test plan afronden • Proof of Concept voorbereiden • Proof of Concept bouwen • Gesprekken met bedrijfsbegeleiders • Proof of Concept documenten	70 uur 10 uur 20 uur 20 uur 10 uur 10 uur 30 uur 80 uur 10 uur 20 uur **Totaal: 280**
25-01-2016 t/m 12-02-2106	• Eerste opzet scriptie • Gesprekken met bedrijfsbegeleiders • Scriptie afronden	120 uur 10 uur 10 uur **Totaal: 140**
xx-03-2016	• Presentatie voorbereiden • Presentatie presenteren	29 uur 1 uur **Totaal: 30**

Risico’s

Aan elk project dat er uitgevoerd word zitten natuurlijk risico’s. Om de risico’s zo goed mogelijk proberen te vermeiden is er een globale planning gemaakt, zie hoofdstuk ‘Globale Planning’. Ook bij dit project kunnen er zich een aantal risico’s voordoen. Hieronder, in tabel 15, ziet u een aantal risico’s die zich kunnen voordoen tijdens dit project:

TABEL 15; RISICO'S

Risico	Maatregel
Ontwerp past niet in de huidige infrastructuur	• Ontwerp aanpassen • Beheerplan wijzigen en de juiste eisen hierin verwerken.
Onduidelijkheid over het beheer	• Beheerplan aanpassen en duidelijk maken hoe het beheer moet worden gedaan.
Tijd tekort bij een eind product	• Extra uren inplannen en eventueel deadline proberen uit te stellen.
Benodigde resources zijn niet beschikbaar	• Planning aanpassen en bekijken hoelang het duurt voordat de resources beschikbaar zijn. • Alternatief zoeken om de resources ergens anders vandaan te halen.
Product voldoet niet aan de eisen van de klant	• Alternatieven zoeken voor het product. • Gesprek met begeleiders en eisen goed in kaart brengen. • Kans op uitloop van de stage, dus extra tijd aanvragen.
Bij een aanval op de externe (front-end) firewall leidt de interne (backend) firewall hier ook onder	• Goede scheiding maken tussen de verschillende netwerken. • In kaart brengen waar het externe verkeer het interne netwerk bereikt. • Aanpassingen maken in de verschillende netwerken.
Het product loopt vast tijdens hoge verkeersdrukte	• Redundant uitvoeren (back-up server) van het product • Het verkeer evenredig verdelen tussen de twee servers.

Persoonlijke uitdagingen

Omdat het voor de student de eerste keer is dat er een project van deze omvang in zijn eentje wordt uitgevoerd is het een uitdaging voor mij om dit project zo soepel mogelijk te laten verlopen. Ook het schrijven van de scriptie is voor mij een uitdading omdat er tijdens de studie niet echt een goede voorbereiding is geweest over hoe je een scriptie moet schrijven. Tijdens de projecten op school wordt er vaak in een team verband gewerkt. Tijdens het afstuderen zal de student alles individueel moeten doen en dit op een zo duidelijk mogelijke manier moeten beschrijven. Omdat het een technisch project is ben ik zeer benieuwd of de dingen die ik geleerd heb tijdens mijn studie tijdens dit project van toepassing zullen zijn. De afstudeeropdracht is een opdracht waar ik zeer naar uitkijk en ik hoop dat ik de opdracht zo soepel en goed mogelijk kan uitvoeren.

Bibliografie

B.V., S. (sd). *Sentia B.V*. Opgeroepen op juni 2015, van Sentia B.V: https://www.sentia.com/

Dobbelaar, C. (2015, Juni 11). CTO. (R. Badal, Interviewer)

Steenhouder, M. (sd). *Leren Communiceren.* Wolters Noordhof.

Bijlage 3: Onderzoeksrapport

Sentia B.V

Onderzoeksrapport

Vak-code: Afstuderen (TICT-AFSTUD-12)

Klas: SV3A

Versie: 1.0

Datum: 11-11-2015

R. Badal 1607426 ricky.badal@student.hu.nl

Onderzoeksrapport, Utrecht, 5-1-2016

R. Badal

Versiebeheer

Hieronder volgt het versiebeheer.

Versie	Datum	Opmerkingen
0.1	11-11-2015	Origineel document opgesteld.
0.2	27-11-2015	Feedback Jos verwerkt.
0.3	01-12-2015	Extra hoofdstukken aangemaakt en lay-out wijzigingen toegepast.
0.4	02-12-2015	Bronverwijzingen aangemaakt en hoofdstukken toegevoegd.
0.5	16-12-2015	Feedback Camiel verwerkt en advies gegeven.
0.6	22-12-2015	Overig commentaar verwerkt.
0.7	24-12-2015	Commentaar Jos verwerk en indeling aangepast.
0.8	05-01-2016	Aanpassingen lay-out gemaakt en commentaar verwerk.
0.9	25-01-2016	REQ-pakketten vervangen door SYN-pakketten.
1.0	25-01-2016	Kosten bijgevoegd.
1.1	27-01-2016	Huidige situatie en gewenste situatie aangepast.
1.2	03-02-2016	Commentaar Jos verwerkt.

Inhoudsopgave

Inleiding

In dit document zullen de onderzoeksresultaten worden beschreven die de student tijdens zijn onderzoeksfase opgedaan heeft. Er zal onderzoek gedaan worden naar het ontwerpen van een virtuele firewall in een bestaande omgeving.

De omgeving waarin de firewall ontworpen zal worden, en het bedrijf momenteel gebruikt, is een VMWare ESXi 5.5 (virtuele) omgeving.

De student zal verschillende pakketten onderzoeken en kijken welk pakket/software het best past in de huidige omgeving van het bedrijf. De pakketten dienen compatibel te zijn met de huidige infrastructuur en technieken die er binnen het bedrijf gebruikt worden.

Doelstelling

In dit onderzoeksrapport zullen de onderzoeksresultaten van de onderzoeksfase worden gedocumenteerd. Om de resultaten goed te kunnen documenteren zal de student verschillende interviews houden en onderzoek doen naar verschillende typen virtuele firewalls op basis van literatuurstudies en praktijktesten.

De student zal onderzoeken aan welke eisen de nieuwe virtuele firewall moet voldoen en welke type virtuele firewall er het beste past in de huidige infrastructuur van het bedrijf.

In dit document zal er een long list en een short list worden toegevoegd op basis van pakketselectie. Aan deze long list en short list zullen functies worden toegevoegd welke er noodzakelijk zijn om te kunnen functioneren in het bestaande netwerk van het bedrijf.

De short list zal een pakketselectie zijn van de longlist. In de longlist komen verschillende type virtuele firewalls te staan met hun functies. In de shortlist zal er gekeken worden welke producten uit de longlist het best passen in het bedrijf en welke pakketten er aan de eisen van de klant voldoen.

Huidige situatie (As Is)

In dit hoofdstuk zal er kort worden beschreven wat de huidige situatie is van het bedrijf en wat voor software het bedrijf gebruikt om hun services aan te bieden aan hun klanten. In het huidige netwerk maakt Sentia gebruik van VMware ESXi 5.5 als hypervisor. VMWare ESXi is een stuk software(besturingssysteem) dat het in staat stelt om virtuele machines op een fysieke machine te creëren en te beheren. VMWare ESXi wordt geïnstalleerd op een fysieke machine als besturingssysteem.

ESXi is een licht besturingssysteem, hierdoor trekt het niet te veel resources van de fysieke machine. Op deze manier blijven er genoeg resources over voor de virtuele machines en kunnen er meerder virtuele machines naast elkaar draaien zonder dat de fysieke machine te veel belast wordt. De virtuele machines hebben hun eigen operating system. Hierdoor kunnen de virtuele machines zich gedragen als 'echte' fysieke servers en kunnen deze virtuele machines gebruikt worden om bijvoorbeeld services aan te bieden (web/ftp/database).

Sentia biedt virtuele omgevingen aan klanten. Deze omgevingen draaien apart van elkaar voor elke klant. De klanten kunnen dus niet bij het netwerk van een andere klant komen. De reden hiervoor is dat elke omgeving van de klant geïsoleerd is door een virtuele firewall. Deze firewall zorgt ervoor dat klant-omgevingen gescheiden blijven. De hoofdtaak van de firewall is het zorgen voor de routering en de filtering van pakketten. De firewall is redundant uitgevoerd. Mocht er een firewall uitvallen, dan wordt de back-up firewall ingeschakeld.

Om ervoor te zorgen dat de virtuele omgevingen bereikbaar zijn via het internet wordt het subnet van de klant via het routeringsprotocol OSPF van de firewalls naar de routers, die met het internet verbonden zijn, gestuurd. De routers sturen dit subnet weer door naar het internet via het BGP-protocol en zo worden de klant omgevingen bereikbaar via het internet.De firewall zorgt dus voor veel taken, waaronder de services die het bedrijf aanbiedt aan de klanten.

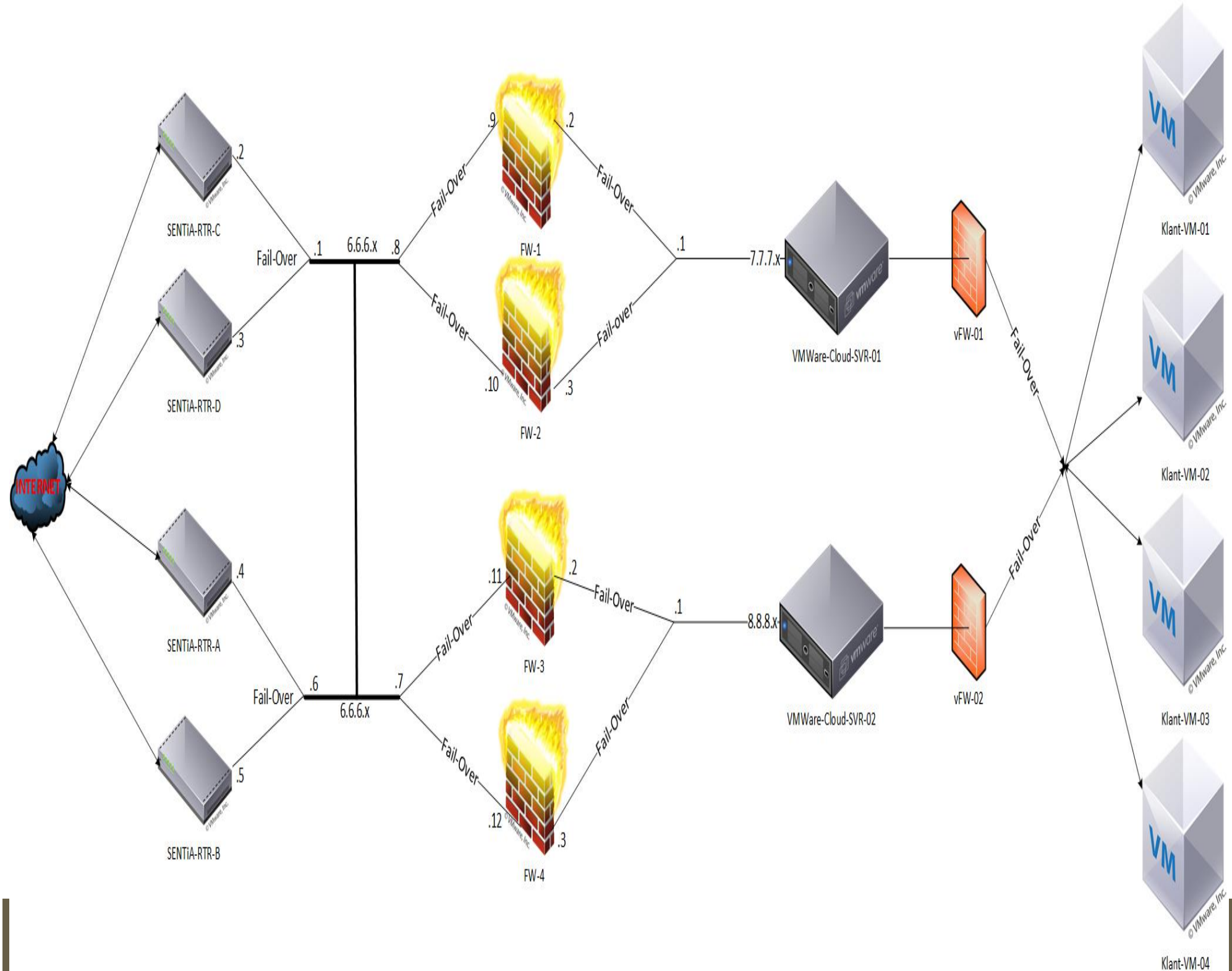
In de huidige situatie wordt er Linux gebruikt als virtuele firewall. Deze firewall stelt het in staat om netwerken te beveiligen en maakt gebruik van de Linux firewall kernel module om pakketten te filteren. Om de verschillende netwerken te beveiligen wordt er gebruik gemaakt van het programma ‘IPTables’. IPTables is een command-line programma voor Linux die de regels toepast in de firewall kernel module. Om firewall rules te beheren dienen er via de command-line commando’s uitgevoerd te worden en dient er kennis te zijn van het programma IPTables om de structuur van de verschillende rules te begrijpen.

Het bedrijf heeft de wens voor een onderzoek, gevolgd door een advies, van verschillende firewalls en functies die aan de eisen en wensen van het bedrijf voldoen en in de huidige infrastructuur passen. Voor een overzicht van de eisen en wensen wordt men doorverwezen naar het hoofdstuk ‘Eisen en wensen’. Aan het eind van het onderzoek zal er een advies plaats vinden waarin duidelijk wordt gemaakt welk pakket er het beste past in de huidige infrastructuur en voldoet aan de eisen en wensen van het bedrijf.

De reden voor dit onderzoek is dat het bedrijf op gestructureerde wijze wilt zien wat de best mogelijke back-end firewall is voor het bedrijf. Met 'best mogelijke' wordt er bedoeld dat de firewall moet voldoen aan de eisen en wensen die het bedrijf stelt. Het pakket dat het hoogste scoort in de vergelijkingstabel (zie *short-list*, pagina 28) kan het best mogelijke pakket zijn. Aan het einde van het onderzoek zal er een conclusie plaats vinden welk pakket/pakketten er het beste zijn en deze conclusie zal gevolgd worden door een advies, welke beschreven zal worden in de scriptie van de student.

Om deze reden is er een project gestart, de afstudeeropdracht van de student, om te onderzoeken welke firewall het beste in de huidige omgeving van het bedrijf past.

In afbeelding 22 ziet men een schets van het netwerk en de services die het bedrijf biedt aan haar klanten;


INTERNET
SENTiA-RTR-C
SENTiA-RTR-D
SENTiA-RTR-A
SENTiA-RTR-B
.2
.3
.4
.5
Fail-Over
.1
6.6.6.x
.8
.6
.7
6.6.6.x
Fail-Over
FW-1
FW-2
FW-3
FW-4
.9
.10
.11
.12
.2
.3
.1
.2
.3
Fail-Over
7.7.7.x
8.8.8.x
VMWare-Cloud-SVR-01
VMWare-Cloud-SVR-02
vFW-01
vFW-02
Fail-Over
Klant-VM-01
Klant-VM-02
Klant-VM-03
Klant-VM-04

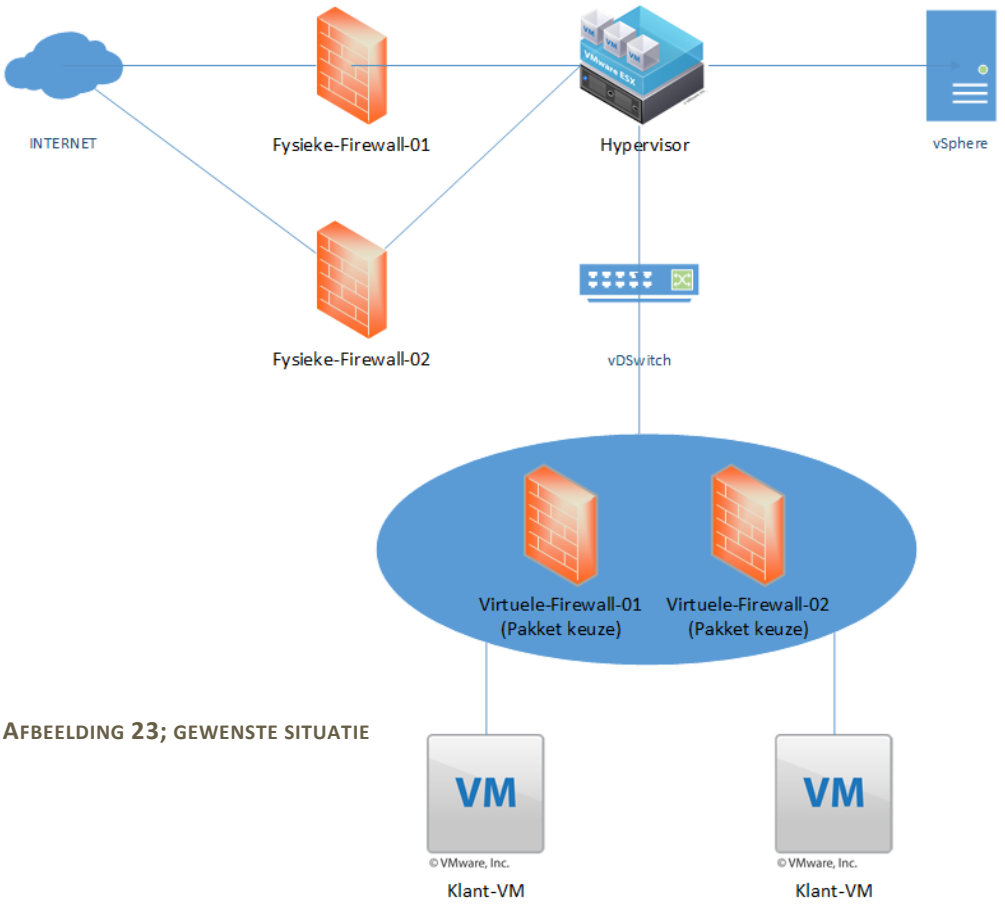
In afbeelding 22 ziet men hoe de routering en de services aangeboden worden naar het internet. Op de VMWare-Cloud servers draaien de virtuele machines van de klanten. Dit kunnen bijvoorbeeld applicatie/web/database/ftp-servers zijn.

Het huidige verkeer wordt geregeld door de virtuele firewalls (vFW-01 en vFW-02 in afbeelding 1). Als twee machines met elkaar willen communiceren, dan moet het verkeer dus eerst naar de firewall, en vervolgens kan het naar de VM/netwerk waar het voor bedoeld is.

Gewenste situatie

In de gewenste situatie zal de virtuele firewall (vFW-01 en vFW-02) vervangen worden door een ander pakket. Het bedrijf heeft een aantal eisen en wensen waardoor het beheer en de functionaliteit van de firewall beter te overzien zijn. De firewall dient beheerbaar te zijn voor medewerkers weinig verstand hebben van de firewall. Voor een volledig overzicht van de eisen en wensen wordt men doorverwezen naar het hoofdstuk ‘Eisen en wensen’.

Een overzicht van de gewenste situatie vindt men in afbeelding 23. De virtuele firewall zal nog steeds dubbel worden uitgevoerd (om de beschikbaarheid te verhogen) en de firewall zal voor dezelfde taken zorgen als in de huidige situatie. Echter zal de nieuwe virtuele firewall aan de eisen en wensen van het bedrijf moeten voldoen.



AFBEELDING 23; GEWENSTE SITUATIE

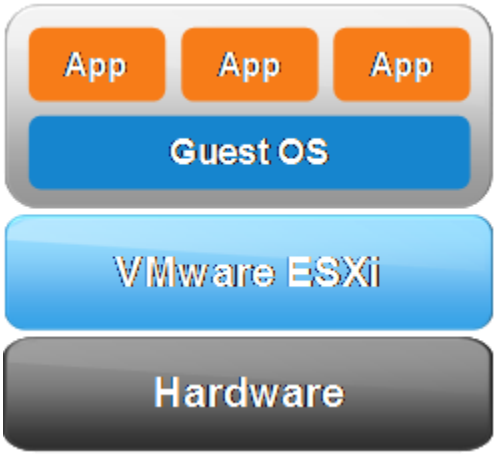
Theoretisch kader

Dit hoofdstuk is bedoeld ter ondersteuning voor het vaststellen van de eisen voor de firewall. Er zullen verschillende technische begrippen worden uitgelegd en er zal duidelijk worden gemaakt welke firewall functies waarvoor dienen. Dit hoofdstuk is de wetenschappelijke basis van het onderzoek dat het student zal uitvoeren gedurende zijn afstudeerperiode bij het bedrijf.

Hypervisor

Een hypervisor is een fysieke machine/server waarop een licht besturingssysteem wordt geïnstalleerd. Een hypervisor stelt het in staat om op een fysieke machine, virtuele machines te creëren en te beheren. Hierdoor kunnen er meerdere machines/besturingssystemen op dezelfde fysieke machine draaien.

Als hypervisor wordt er binnen het bedrijf gebruikgemaakt van VMWare ESXi versie 5.5. VMWare ESXi is een licht besturingssysteem dat maar 3-400 Mb groot is. Het gebruikt dus niet veel resources van de fysieke machines, hierdoor blijven de resources beschikbaar voor de virtuele machines. In afbeelding 24 ziet men een schets hoe een hypervisor werkt;



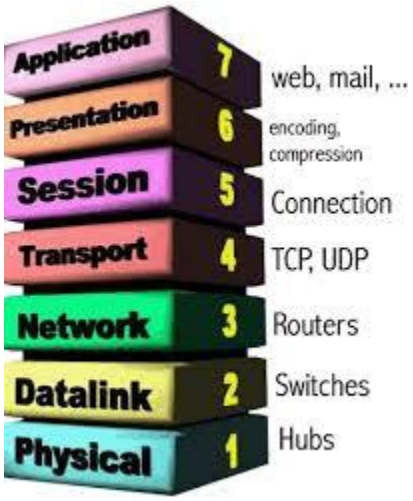
AFBEELDING 24; HYPERVISOR (VMWARE, 2009)

In afbeelding 24 ziet men dat VMWare ESXi op de hardware draait. In VMWare ESXi kunnen er verschillende virtuele machines worden aangemaakt met elk hun eigen besturingssysteem (Guest OS). Op deze virtuele machines kunnen verschillende applicaties draaien, bijvoorbeeld een web/ftp/file server. (WikiPedia, 2015)

Netwerk virtualisatie

Netwerk virtualisatie houdt in dat er logische, virtuele netwerken gecreëerd kunnen worden die onafhankelijk op elk type hardware kunnen draaien. Met netwerk virtualisatie kunnen de fysieke netwerken gevirtualiseerd worden. Hierdoor hoeft er geen aparte hardware worden gekocht voor een router/switch en hoeven er geen fysieke computers aan geschaft te worden om als server te dienen voor het bedrijf.

De verschillende services die normaal fysiek worden aangeboden, zoals; storage, firewall of fysieke switches en/of routers kunnen dus allemaal gevirtualiseerd worden. Er is in theorie maar één fysiek apparaat nodig, de hypervisor, om alle (netwerk)componenten te kunnen virtualiseren. Virtualisatie geldt voor alle 7 lagen van het OSI-model; een voorbeeld van het OSI-model ziet men in afbeelding 25 hieronder;



AFBEELDING 25; OSI MODEL (IDEMDITO, 2005)

Door middel van netwerk virtualisatie kunnen dus alle 7 lagen van het OSI-model gevirtualiseerd worden. Dit houdt in dat applicaties zoals web en mailserver ook virtueel gecreëerd kunnen worden en onderdeel zijn van het virtuele netwerk.

Firewall

Een firewall is een stuk software dat het in staat stelt om een netwerk/netwerken te controleren op het verkeer wat erin en eruit gaat. Er kunnen verschillende dingen geblokkeerd worden tussen netwerken. Een firewall kan op verschillende manieren in een netwerk worden geplaatst. Zo kan er op een firewall bijvoorbeeld worden ingesteld dat netwerk-A, netwerk-B niet mag bereiken, maar netwerk-B mag netwerk-A wel bereiken.

Er zijn veel verschillende typen firewalls. Een overzicht van de verschillende type firewalls vindt men hieronder;

Packet filtering firewall

Een packet filtering firewall kijkt op laag 4 van het osi-model (de TCP/IP laag). Door middel van rules te creëren wordt er gekeken of een IP-pakket wordt toegelaten of afgewezen. Ook kijkt deze type firewall naar de destination port en source IP-adres. Een packet filtering firewall kan bijvoorbeeld al het verkeer naar de SSH port (23) verbieden. Het protocol zelf (SSH) kan niet worden geblokkeerd. Als SSH dus op een andere port draait, kan er nog steeds een connectie worden opgezet.

Application layer firewall

Een aplication layer firewall kan ook op applicatie niveau (zoals de naam als zegt) functioneren. Er wordt in eerste instantie ook op de TCP/IP laag gekeken, vervolgens bepaald een stukje software of de pakketten worden doorgelaten of tegen worden gehouden. Bij een applicatie layer firewall wordt er op protocol niveau gekeken. Zo kan bijvoorbeeld SSH op een andere poort alsnog worden geblokkeerd.

Stateless firewall

Dit is een firewall dat elk pakketje dat binnen het netwerk komt individueel behandelt. Er wordt geen informatie opgeslagen over bijvoorbeeld een SYN-pakket(request) en een ACK-pakket(akkoord). Dit betekent dus dat er geen connectie wordt gelegd als er nog een ACK moet worden teruggestuurd. Deze type firewall wordt niet vaak in het bedrijfsleven gebruik.

Statefull firewall

In tegenstelling tot de stateless firewall, houdt de statefull firewall wel informatie bij. Er wordt dus wel gekeken als er bijvoorbeeld een SYN-pakket (request) komt, of er voor diezelfde sessie ook een ACK-pakket (akkoord) weggaat. Zo kan de firewall sessie informatie bijhouden.

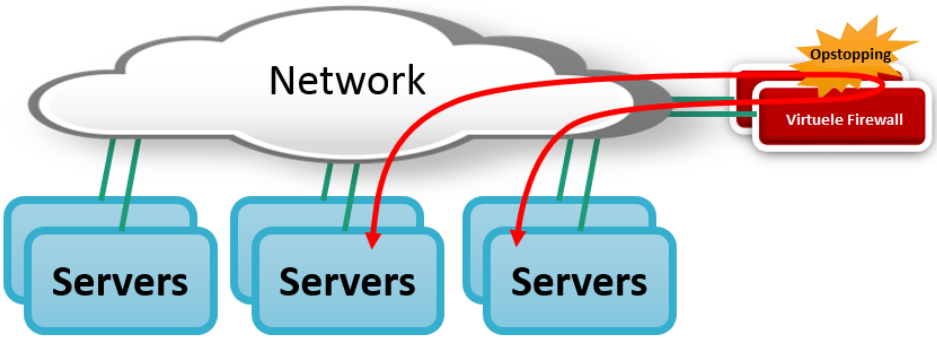
De variant statefull firewall zal toegepast worden in de huidige infrastructuur van het bedrijf omdat deze variant de optie heeft om sessie informatie van verkeer bij te houden. Het dataverkeer tussen zender en ontvanger wordt inhoudelijk geanalyseerd en er wordt verder dan alleen het IP-adres en het poortnummer gekeken. De inhoud van de pakketjes worden bekeken en op basis van de inhoud kunnen de pakketjes dan verschillend behandeld worden: toegestaan, geweigerd, of met een andere prioriteit worden doorgestuurd.

Distributed firewall

Bij een gedistribueerde firewall zit de firewall geïmplementeerd in de hypervisor. Hierdoor is er geen aparte virtuele machine nodig die voor de firewall rol zorgt. Alle machines die op de hypervisor zijn aangemaakt zijn bekend bij een gedistribueerde firewall. Dit maakt het mogelijk om voor elke virtuele machine een eigen aparte virtuele firewall te creëren. Zo kan elke klant dus zijn/haar eigen firewall hebben.

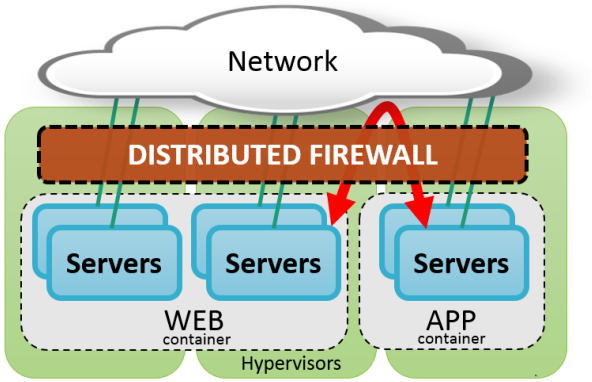
Bij een virtuele firewall wordt er een virtuele machine aangemaakt en worden de machines die beschermd moeten worden aangesloten op de virtuele firewall. Als een machine dus niet aangesloten zit op de firewall, dan heeft deze machine geen bescherming.

Hieronder in afbeelding 26 ziet men een voorbeeld van een virtuele firewall en het gevaar waardoor het netwerk zich kan ophopen.



AFBEELDING 26; VIRTUELE FIREWALL (VMWARE, FIREWALL, 2013)

In afbeelding 27 ziet men een voorbeeld van een gedistribueerd firewall. In deze omgeving maakt de firewall deel uit van de hypervisor. Er hoeft dus geen aparte virtuele machine aangemaakt te worden om als firewall te functioneren. Dit heeft als voordeel dat de gedistribueerde firewall meer resources ter beschikking heeft en kennis heeft van elke virtuele machine die geïnstalleerd is op de hypervisor. Op deze manier kan er voor elke virtuele machine een aparte virtuele firewall worden gecreëerd. (FAQs, 2013)



AFBEELDING 27; GEDISTRIBUEERDE FIREWALL (VMWARE, FIREWALL, 2013)

Software Defined Networking

Software Defined Networking (SDN) is een architectuur die het in staat stelt om dynamisch met netwerken om te gaan. Door middel van SDN kan een netwerk 'geprogrammeerd' worden en kunnen er templates gemaakt worden van standaard netwerken. Zo kan er bijvoorbeeld een template worden gemaakt van een netwerk dat bestaat uit de volgende onderdelen;

- Router
- Switch
- DHCP-server
- Web-server

Omdat dit type netwerk gebruikt kan worden voor verschillende klanten kan hier een template van worden gemaakt en kan dit voor elke klant automatisch worden uitgerold. SDN stelt het in staat om verschillende netwerken op een centrale plek te beheren door middel van een SDN Controller. Op deze controller zijn alle netwerken zichtbaar en kunnen er firewall rules worden aangemaakt voor de verschillende netwerken. De architectuur die SDN gebruikt voldoet aan de volgende functies;

- Direct programmeerbaar; Netwerken kunnen geprogrammeerd worden en kunnen automatisch worden uitgerold.
- Dynamisch; De verschillende netwerken kunnen dynamisch worden aangepast. Zo kan het netwerk worden aangepast naar de wensen van de klant
- Centraal beheer; Omdat er in Cloud computing veel servers/services worden aangeboden maakt SDN het mogelijk om alle servers/services centraal te kunnen beheren. Zo heeft een netwerkbeheerder direct overzicht over het gehele netwerk.
- Programmeerbare configuraties; De functies die een netwerk kan bieden zijn door middel van SDN ook programmeerbaar. Zo kan het netwerk of een server automatisch beveiligd worden door middel van standaard firewall regels die automatisch geïntegreerd kunnen worden in een netwerk.
- Open standaarden; Door gebruik te maken van open standaarden kan de SDN-controller geïmplementeerd worden in verschillende omgevingen en is het niet vendor (fabrikant) afhankelijk.

De functies die hierboven staan beschreven komen terug in de eisen en wensen die het bedrijf heeft voor het nieuwe pakket.

Interviews

In dit hoofdstuk zullen de interviews worden beschreven die er hebben plaats gevonden om de eisen en wensen in kaart te brengen voor de opdracht. Een overzicht van het interview is te vinden in tabel 16;

TABEL 16; INTERVIEW - CAMIEL DOBBELAAR/TOM VAN LEEUWEN

Vraag	Antwoord/opmerking
Aan welke eisen dient de nieuwe firewall te voldoen?	Na overleg met Camiel Dobbelaar is de student samen met Camiel op een aantal eisen/wensen gekomen; de eisen/wensen zijn als volgt; *Performance, High Availability, Beheerbaarheid, Automatisering, IPv6 Routering, VXLAN, Open-Source en Quality* en *Service*
Wat is een goede test om de functionaliteit van de nieuwe firewall te testen?	Met het programma 'iPerf' kunnen er TCP-sessies worden opgezet. Het programma kan verschillende parallelle sessies opzetten, hierdoor kan de bandbreedte maximaal getest worden.
Wat dient er geautomatiseerd te kunnen worden?	De firewall rules moeten via een script automatisch ingevoerd kunnen worden. De beheerder hoeft dus niet op de firewall zelf in te loggen om rules aan te maken, dit dient automatisch te kunnen.
Wat wordt er verstaan onder beheerbaarheid?	De firewall dient firewall beheerbaar te zijn zonder een gebruikersinterface, waardoor automatisering mogelijk wordt.

Eisen en wensen

In dit hoofdstuk zullen de eisen en de wensen worden besproken waaraan het uiteindelijke product zal moeten voldoen. Deze eisen en wensen zijn in kaart gebracht door verschillende literatuurstudies en interviews die gehouden zijn met de technische medewerkers van het bedrijf. Op basis van deze eisen en wensen zal er een longlist en een shortlist worden gecreëerd. In tabel 173 hieronder ziet men een overzicht van de eisen en wensen;

TABEL 17; EISEN EN WENSEN

Type	Functionele eis/wens	Beschrijving
Wens	Open Source	Omdat het bedrijf veel met open source producten werken, heeft het bedrijf de wens dat de firewall ook open source is. Dit is niet noodzakelijk, vandaar dat dit als wens genoteerd is.
Eis	Performance	De nieuwe firewall dient niet meer dan 70% CPU te verbruiken bij een routering van 1 Gbit/s.
Eis	High Availability	De virtuele firewall dient High Availability te ondersteunen. Dit houdt in dat een back-up firewall de taken over dient te nemen, met behoud van de sessie tabel, als de hoofd firewall uitvalt.
Eis	IPv6 routering	Omdat de IPv4 adressen opraken is het een eis dat de nieuwe virtuele firewall IPv6 adressen kan routeren.
Eis	VXLAN	Omdat er in de huidige infrastructuur gebruik gemaakt wordt van VLAN's is er een limit (4096) op het aantal VLAN's. VXLAN haalt dit limiet weg en stelt het in

		staat om VLAN's op laag 2 en 3 te koppelen.
Wens	QoS	Om bepaald verkeer voorrang te geven is het de wens dat de nieuwe firewall pakketten kan prioriteren, zodat er voorrang verleend kan worden aan een bepaalde verkeersstroom.
Wens	Distributed Firewall	Een distributed firewall maakt het mogelijk om beveiligingen toe te passen op een hoger niveau dan alleen netwerkniveau. Bijvoorbeeld op serveniveau binnen een netwerk.
Eis	Beheerbaarheid	De nieuwe firewall dient eenvoudig beheerbaar te zijn voor medewerkers die geen verstand hebben van de firewall. Zo dienen firewall functies programmeerbaar te zijn voor de firewall.
Eis	Integratie met de huidige infrastructuur	De nieuwe firewall dient compatibel te zijn met de huidige infrastructuur. Er hoeven dus niet veel wijzigingen plaatst te vinden om de firewall te implementeren in de huidige infrastructuur.
Eis	Automatisering	De firewall dient zodanig compatibel te zijn dat het API's ondersteunt. Op deze manier kunnen er netwerken automatisch worden uitgerold.

MoSCoW Analyse

Met de eisen en wensen eenmaal in kaart gebracht kan er een MoSCoW analyse plaats vinden op deze eisen en wensen om zo prioriteiten te stellen tussen de eisen en wensen. In deze paragraaf bevindt zich een MoSCoW analyse gebaseerd op de eisen en wensen van het bedrijf. Tijdens deze analyse worden de eisen en wensen als volgt gecategoriseerd;

- M - Must haves; vereist om het product werkbaar aan te kunnen tonen.
- S - Should haves; wenselijke eisen, niet vereist
- C - Could haves; Functies die meegenomen kunnen worden, maar niet noodzakelijk zijn
- W – Won't haves; Functies die niet meegenomen worden, maar in de toekomst wel geïmplementeerd kunnen worden

In tabel 18 ziet men een overzicht van de MoSCoW analyse;

TABEL 88; MOSCOW ANALYSE

Eis/Wens	Must have	Should have	Could have	Won't have
Performance/Multi-CPU	X			
High Availability	X			
Beheerbaarheid (Centraal)	X			
Automatisering	X			
Monitoring	X			
IPv6 routering		X		
VXLAN		X		
Open source		X		
Distributed firewall		X		
QoS			X	

Longlist

In de longlist zullen pakketten worden geselecteerd op basis van de eisen en wensen van het bedrijf. Deze lijst is tot stand gekomen na overleg met het bedrijf en na het vaststellen van de MoSCoW analyse. Er is onderzoek gedaan op basis van literatuurstudies naar de verschillende pakketten en functies van deze pakketten. Uit de longlist zullen er een aantal pakketten in aanmerking komen van de shortlist. De shortlist is een specifiekere lijst waarin de pakketten specifiek getest kunnen worden. De pakketten die meegenomen zijn in de long list zijn als volgt;

- pfSense
- VMWare NSX
- Untangle
- IPCop
- Smoothwall
- OPNSense
- Contrail

Deze pakketten zijn individueel vergeleken met elkaar op basis van de MoSCoW analyse. Een overzicht van de vergelijkingen van de pakketten vindt men in tabel 19;

TABEL 99; LONGLIST

Product	High Availability (*Must*)	Performance	Centraal management (*Must*)	Automatisering (*Must*)	Open-source (*Should*)	IPv6 (*Should*)	Distributed firewall (Should)	VXLAN (*Should*)	QoS (*Could*)
pfSense	Ja	Ja	Ja	Ja/EasyRule	Ja	Ja	Nee	Ja	Ja
VMWare NSX	Ja	Ja	Ja	Ja/REST API's	Nee	Ja	Ja	Ja	Ja
Untangle	Ja	Ja	Ja	Nee	Ja	Ja	Nee	Ja	Ja
IPCop	Ja	Ja	Ja	Nee	Ja	Ja	Nee	Ja	Ja
Smoothwall	Niet standaard	Ja	Ja	Nee	Ja	Ja	Nee	Ja	Ja
OPNSense	Ja	Ja	Ja	Nee	Ja	Ja	Nee	Ja	Ja
Contrail	Ja	Ja	Ja	Ja/REST API's	Ja	Ja	Ja	Ja	Ja

Shortlist

Uit de longlist zijn er een aantal producten afgevallen omdat deze niet aan alle wensen en eisen van het bedrijf voldoen. Een shortlist dient als lijst die de producten uit de longlist haalt die het best als oplossing komen uit de lijst in combinatie met de eisen en wensen van de klant.

Uit de longlist zijn er drie producten gekomen die aan de meeste eisen en wensen van de klant voldoen. De producten die in de shortlist komen ziet men in tabel 20;

TABEL 20; MOSCOW ANALYSE OP PRODUCTEN

Product	High Availability (*Must*)	Performance	Centraal management (*Must*)	Automatisering (*Must*)	Open-source (*Should*)	IPv6 (*Should*)	Distributed firewall (Should)	VXLAN (*Should*)	QoS (*Could*)
pfSense	Ja	Ja	Ja	Ja/EasyRule	Ja	Ja	Nee	Ja	Ja
VMWare NSX	Ja	Ja	Ja	Ja/REST API's	Nee	Ja	Ja	Ja	Ja
Contrail	Ja	Ja	Ja	Ja/REST API's	Ja	Ja	Ja	Ja	Ja

De drie producten die in de shortlist staan worden meegenomen in het Proof of Concept. De studenten zal de drie producten in een test opstelling opbouwen en er zullen verschillende testen worden gedaan om te kijken welk product er het best past in de huidige omgeving van het bedrijf, een VMWare ESXi 5.5 omgeving. De pakketten zullen getest worden in de testomgeving die de student heeft opgebouwd.

Kosten

In deze paragraaf zullen de kosten worden besproken die gekoppeld zijn aan de pakketten. Omdat niet alle pakketten 'closed-source' pakketten zijn (betaalde pakketten) zullen er verschillen plaats vinden in de kosten van de pakketten. De pakketten die in dit hoofdstuk besproken zullen worden zijn de pakketten die uit de 'short-list' zijn gekomen tijdens de onderzoeksfase. De pakketten zijn als volgt;

- pfSense
- VMWare NSX
- Contrail

Een overzicht van de kosten kan men vinden in tabel 21;

TABEL 21; KOSTEN PAKKETTEN SHORT-LIST

Product	Kosten aanschaf	Kosten support
PfSense	€0,- (Open-source)	€0,- (community based support)
VMWare NSX	20 punten per beheerde VM*	Inbegrepen bij de aanschaf kosten
Contrail	€0,- (Open-source)	

Omdat 'open-source' geen MUST is in de MoSCoW analyse, vallen de pakketten waarvoor betaald moeten worden niet af. Op de manier kan er een goede vergelijking worden gedaan tussen de betaalde pakketten en de gratis pakketten.

**Sentia heeft een VMWare licensing van 5 punten per GB(RAM) per maand. Er wordt alleen gekeken naar het geheugen wat er in gebruik is. Als een machine bijvoorbeeld 4GB geheugen heeft, en er wordt maar 2 GB gebruikt, dan worden de kosten alleen over de 2GB berekend. Voor een NSX-installatie worden er 20 punten per maand per virtuele machine die in beheer is van het pakket(NSX) berekend. 1 punt is ongeveer 80 cent. Deze kosten zijn gebaseerd op de VMWare vCAN Guide 2015 Q2.*

Testomgeving

Omdat het onderzoek en het testen niet in een productie omgeving plaats kan vinden heeft de student een testopstelling gecreëerd. De testopstelling bestaat uit twee fysieke machines. Eén van de machines simuleert de VMware ESXi 5.5 omgeving waarop de omgeving van de klanten draait. De andere fysieke machine simuleert de fysieke OpenBSD firewall.

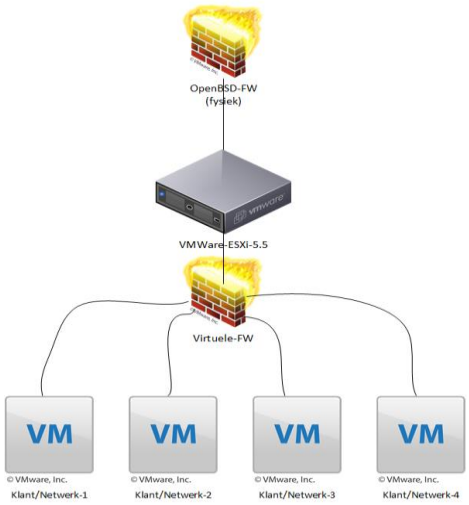
Om de testresultaten zo veel mogelijk hetzelfde te houden heeft de student ervoor gekozen om de productie omgeving na te bouwen als een testomgeving. De VMWare ESXi 5.5 machine is de hypervisor. Hierop draait dezelfde software als in de productie omgeving. Ook op de tweede fysieke machine, de OpenBSD firewall, draait dezelfde software als in de productie omgeving.

Op deze manier kan de student het netwerk ongeveer hetzelfde houden en worden de testresultaten niet beïnvloedt door een software conflict.

Op de VMWare ESXi 5.5 machine draaien 4 virtuele machines. Deze virtuele machines staan elk apart in een ander netwerk (dit simuleert de verschillende klant omgevingen). In de huidige situatie is er als virtuele firewall op de VMWare ESXi 5.5 machine gekozen voor dezelfde software als de fysieke firewall, OpenBSD versie 5.

Deze virtueel firewall presteert niet goed in bepaalde situaties (als promiscuous-mode aan staat voor High Availability) en kan hierdoor zijn hoofdtaak, het routeren en filteren van pakketten, niet meer goed uitvoeren.

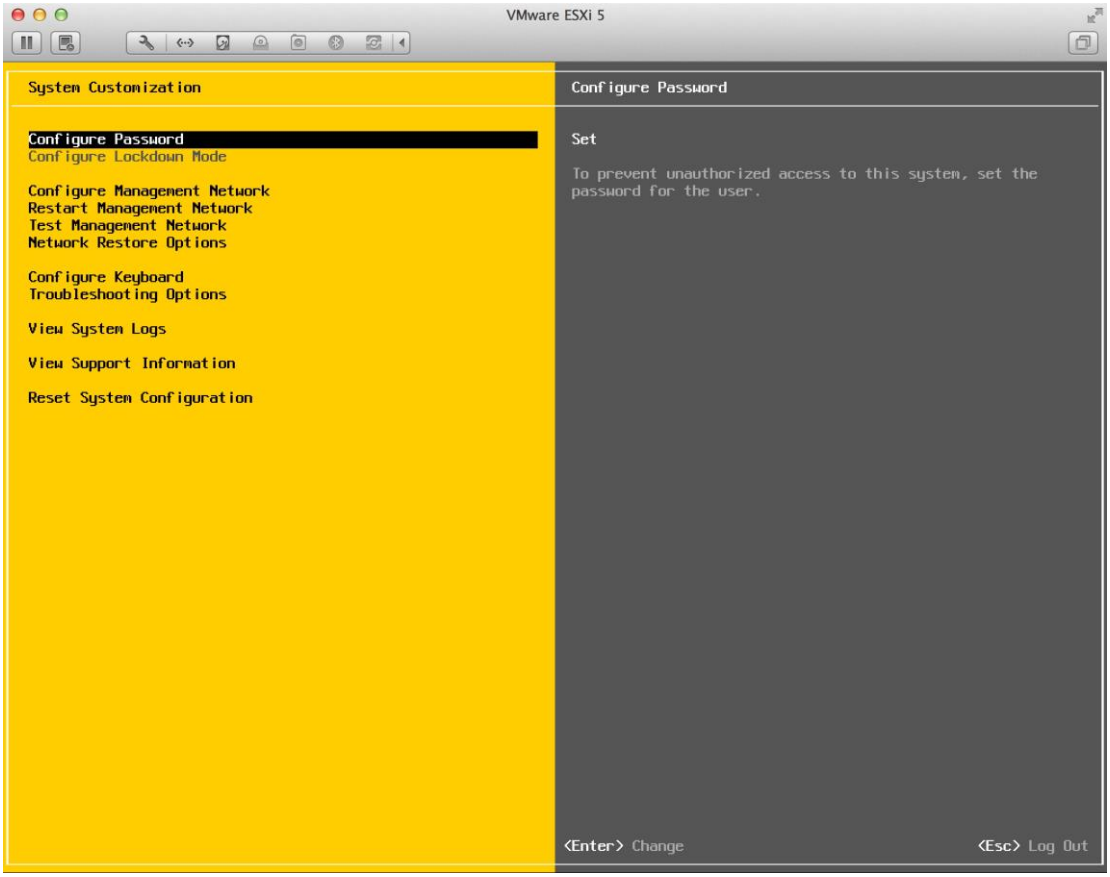
Het is aan de student om te onderzoeken welke virtuele firewall er het best presteert in een virtuele omgeving en welke type virtuele firewall het best in de bestaande infrastructuur past. Hieronder, in afbeelding 28, ziet men een netwerktekening van de testomgeving die de student gecreëerd heeft;



AFBEELDING 28; TESTOPSTELLING (B.V, 2015)

VMWare ESXi

Zoals er in het hoofdstuk ‘Huidige situatie’ staat beschreven draaien de virtuele machines van de klant op een server(hypervisor) met daarop VMWare ESXi geïnstalleerd. VMWare ESXi maakt het mogelijk om verschillende netwerken en virtuele machines te creëren en te beheren. Als VMware ESXi eenmaal geïnstalleerd is op de hypervisor dan kan de hypervisor beheerd worden door een externe applicatie. Met fysieke toegang tot de hypervisor kunnen er geen virtuele machines/netwerken gecreëerd worden. Er kunnen een basis aantal dingen worden ingesteld zodat er connectie gemaakt kan worden met de externe applicatie genaamd vSphere Client. In afbeelding 29 ziet men de opties die er in te stellen zijn met fysieke toegang tot VMWare ESXi;

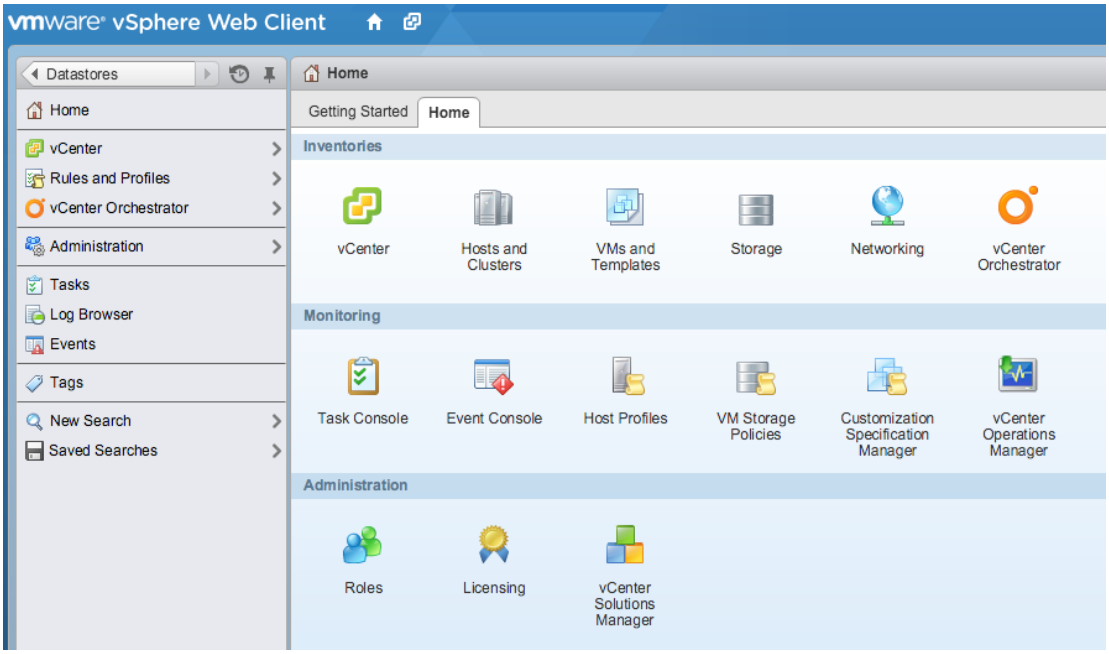


AFBEELDING 29; ESXI OPTIES (SYSADMINTUTORIALS, 2006)

Als het netwerk eenmaal goed is ingesteld dan kan de hypervisor beheerd worden met de vSphere Client. Via de vSphere Client kunnen er virtuele machines en netwerken worden gecreëerd en worden beheerd.

vCenter Server Appliance

Als de hypervisor eenmaal goed geconfigureerd is dan kan de hypervisor gemanaged worden door de managing software van VMWare genaamd; vCenter Server Appliance. Deze software stelt het in staat om de hypervisor te managen. Er kunnen virtuele machines, netwerken en switches worden gecreëerd en beheerd. De vCenter Server Appliance kan virtueel op de hypervisor worden geïnstalleerd. De virtuele machine waarop de vCenter Server Appliance software draait heeft minimaal 8 GB RAM nodig om te kunnen functioneren. Als de virtuele machine met de software eenmaal geïnstalleerd is dan kan de hypervisor worden beheerd via een webbrowser. In de browser wordt het IP-adres van de virtuele machines ingetypt waarop de vCenter Server Appliance software is geïnstalleerd. Hieronder in afbeelding 30 ziet men een voorbeeld van de web interface van vCenter Server Appliance;



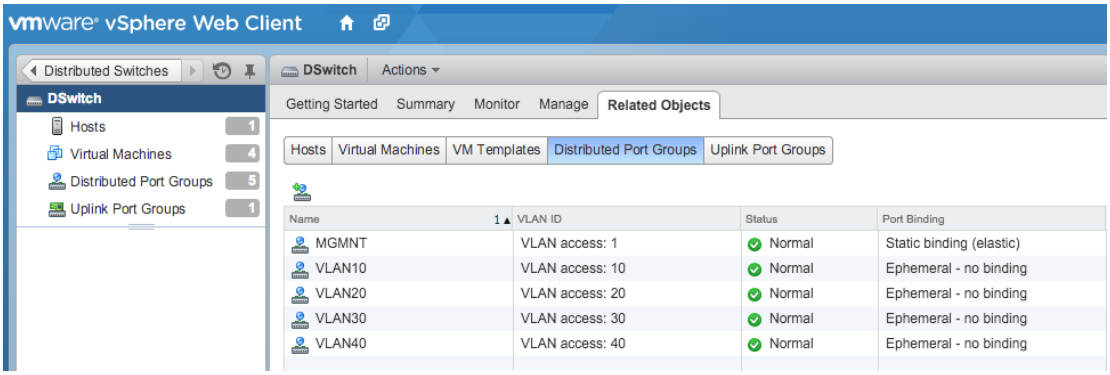
AFBEELDING 30; WEB CLIENT VCENTER SERVER APPLIANCE (SYSADMINTUTORIALS, 2006)

Via de web interface kunnen er verschillende taken worden uitgevoerd. Om de testopstelling zo gelijk mogelijk te houden aan de productie omgeving van het bedrijf heeft de student dezelfde (virtuele) opstelling gecreëerd in zijn testopstelling. Als eerst wordt er een gedistribueerde switch aangemaakt op de hypervisor. Meer hierover is te lezen in de volgende paragraaf; Switching

Switching

Het bedrijf heeft veel verschillende klanten en biedt vele services aan. Om deze services centraal te kunnen beheren heeft het bedrijf een virtuele gedistribueerde switch geïmplementeerd in de virtuele omgeving die het bedrijf biedt aan haar klanten. Een gedistribueerde switch is een switch waar het beheer op een centrale plek wordt gedaan (in dit geval op de hypervisor via de vCenter web interface). Alle netwerken zijn bekend op de gedistribueerde switch en als er een netwerk bij komt dan is dit netwerk gelijk bekend op alle virtuele machines. Een netwerk hoeft dus niet 'doorgetrokken' worden naar verschillende virtuele machines maar is gelijk overal bekend.

Voor de testopstelling heeft de student ook gebruik gemaakt van een gedistribueerde switch. Op deze gedistribueerde switch zijn vier verschillende VLAN's aangemaakt, VLAN 10, 20, 30 en 40. Een VLAN maakt scheiding tussen de verschillende netwerken. Op deze manier kunnen de klanten niet bij elkaar in het netwerk komen. Hieronder, in afbeelding 31, is er een overzicht van de gemaakte VLAN's;



AFBEELDING 31; VLAN'S OP DE GEDISTRIBUEERDE SWITCH (BADAL, ONDERZOEK, 2015)

iPerf

Om de resources van de nieuwe virtuele firewall goed te kunnen testen maakt de student gebruik van het programma 'iPerf'. iPerf is een netwerk bandbreedte applicatie die het in staat stelt om de throughput van het netwerk optimaal te belasten om zo de throughput te testen. iPerf maakt gebruikt van TCP en UDP-connecties. Om het programma goed te testen is er een server en een client nodig. Om de belasting van de virtuele firewall te testen heeft de student een virtuele machine in VLAN 10 en een virtuele machine in VLAN 20. De firewall routeert tussen de twee virtuele machine. Op deze manier wordt de virtuele firewall getest op routering en het verbruik van resources.

Conclusie

Uit de shortlist is gebleken dat er een drietal producten zijn die voldoen aan de eisen van de klant. Er is gekeken naar de '*Must haves'* van de eisen en vervolgens heeft de MoSCoW analyse plaats gevonden op de producten. De producten zijn *Contrail*, van de fabrikant *Juniper*, *NSX* van de fabrikant *VMWare* en het pakket *pfSense.*

Als er gekeken wordt naar de 'Must haves' en de 'Should haves' dan blijven er nog twee producten over, namelijk; Contrail en pfSense. VMWare NSX is het enige product uit de short-list dat geen open-source product is. Omdat open-source een wens is, en geen eis, kan het pakket hierdoor niet afvallen.

De producten maken het mogelijk om virtuele firewalls te creëren en verschillende firewall rules per netwerk op te zetten. Op deze manier heeft de beheerder een duidelijk overzicht over de firewall rules.

Deze drie producten zullen meegenomen worden in het Proof of Concept. Er zal tijdens het Proof of Concept worden gekeken naar de functionaliteit van de producten en de manier waarop de producten integreerbaar zijn in de huidige infrastructuur. Om de pakketten uit de testen maakt de student gebruikt van de testopstelling die de student gebouwd heeft.

Bibliografie

B.V, S. (2015). *Virtual Network.* Nieuwegein: Sentia B.V.

B.V., S. (sd). *Sentia B.V*. Opgeroepen op juni 2015, van Sentia B.V: https://www.sentia.com/

Badal, R. (2014). *NWA_Architectuur_v0.7.* Utrecht: NWA.

Badal, R. (2015, 12 01). Onderzoek. Utrecht, Utrecht, Utrecht.

Dobbelaar, C. (2015, Juni 11). CTO. (R. Badal, Interviewer)

FAQs. (2013, 03 12). *Firewall*. Opgehaald van FAQs: http://www.faqs.org/faqs/firewalls-faq/

IdemDito. (2005, 03 12). *OSI Model*. Opgehaald van TCP: http://server.idemdito.org/svt/techtalk/osi.htm

Steenhouder, M. (sd). *Leren Communiceren.* Wolters Noordhof.

Sysadmintutorials. (2006, 01 03). *Sysadmintutorials*. Opgehaald van VMWare ESXI: http://www.sysadmintutorials.com/tutorials/vmware-vsphere-5-x/esxi-5/configuring-vmware-esxi-5/

VMWare. (2009, 04 23). *Virtualization*. Opgehaald van VMWare: https://blogs.vmware.com/virtualreality/author/eric_horschman/page/2

VMWare. (2013, 07 07). *Firewall*. Opgehaald van Firewall: http://bradhedlund.com/2013/07/07/what-is-a-distributed-firewall/

Wikipedia. (2014, 11 14). *Wikipedia*. Opgehaald van Wikipedia: https://nl.wikipedia.org/wiki/Firewall

WikiPedia. (2015, 11 17). *Hypervisor*. Opgehaald van WikiPedia: https://en.wikipedia.org/wiki/Hypervisor

Bijlage 4: Functioneel Ontwerp

Functioneel Ontwerp

Sentia B.V.

Vak-code: Afstuderen (TICT-AFSTUD-12)

Klas: SV3A

Versie: 1.0

Datum: 27-1-2016

R. Badal 1607426 ricky.badal@student.hu.nl

Functioneel Ontwerp, Utrecht, 27-1-2016

R. Badal

Versiebeheer

Hieronder volgt het versiebeheer.

Versie	Datum	Opmerkingen
0.1	22-12-2015	Origineel document opgesteld
0.2	05-01-2016	Hoofdstukken toegevoegd en indeling aangepast.
0.3	12-01-2016	Commentaar begeleiders verwerkt.
0.4	17-01-2016	Commentaar verwerkt
0.5	19-01-2016	Kosten en beheer toegevoegd.
0.6	25-01-2016	Kosten verplaatst naar het onderzoeksrapport.
0.7	27-01-2016	Eisen en wensen aangepast.

Inhoudsopgave

Inleiding

In dit document zal het Functioneel Ontwerp voor de afstudeeropdracht van de student worden beschreven. Tijdens de onderzoeksfase heeft de student een aantal eisen en wensen in kaart gebracht waaraan het eindproduct moet voldoen. Dit document zal de functies beschrijven die het uiteindelijke pakket zal moeten hebben om aan de wensen en eisen van het bedrijf te voldoen. Ook de architectuur van het nieuwe pakket zal worden beschreven en er zal een visueel overzicht van de architectuur worden opgesteld.

De opdracht die de student zal moeten uitvoeren kan omschreven worden als een ontwerp/advies opdracht. Om de afstudeeropdracht structuur te geven is de opdracht verdeeld in verschillende fases. Het Functioneel Ontwerp is onderdeel van de afstudeeropdracht en maakt deel uit van de *Ontwerpfase*.

De functies waaraan het uiteindelijke pakket aan zal moeten voldoen zullen in dit document beschreven worden en er zal duidelijk worden gemaakt waar de functies voor dienen. Het beheer van het pakket dient ook aan een aantal eisen en wensen te voldoen. Hiervoor zal er een beheerplan worden opgesteld waarin er duidelijk wordt gemaakt welke eisen en wensen er gesteld worden en waarvoor de eisen en wensen dienen. Het beheerplan kan men vinden in het hoofdstuk '*Bijlage - Beheerplan*'.

Doelstelling

Het doel van het Functioneel Ontwerp is om de functies waaraan het pakket moet voldoen in kaart te brengen en een duidelijk beeld te schetsen aan welke functionele eisen het eindpakket moet voldoen. Om de eisen en wensen zo duidelijk mogelijk te beschrijven zullen de eisen en wensen in een apart hoofdstuk worden beschreven en er zal duidelijk worden gemaakt wat de functies zijn van de eisen en waarom dit noodzakelijk is voor het bedrijf.

Beheerplan

De beheerbaarheid van het pakket is een belangrijk onderwerp. Om deze reden zal de student een beheerplan opstellen dat in kaart brengt hoe het nieuwe eindpakket beheerd kan worden. Dit zal in overleg met het bedrijf gedaan worden en er zal goed worden gekeken wat de beste manier is om het eindproduct te beheren. Het beheerplan is te vinden als bijlage in dit document.

Functionele eisen en wensen

In dit hoofdstuk zullen de eisen en wensen in kaart worden gebracht die het bedrijf stelt aan het eindpakket. De eisen en wensen zijn tot stand gekomen na literatuurstudies en het interviewen van verschillende medewerkers van het bedrijf. Hieronder, in tabel 22, is er een overzicht van de eisen en wensen waaraan het pakket zal moeten voldoen;

TABEL 22; EISEN EN WENSEN

Eis/Wens	Must have	Should have	Could have	Won't have
Performance/Multi-CPU	X			
High Availability	X			
Beheerbaarheid (Centraal)	X			
Automatisering	X			
Monitoring	X			
IPv6 routering		X		
VXLAN		X		
Open source		X		
Distributed firewall		X		
QoS			X	

Deze eisen en wensen zijn tot stand gekomen na verschillende interviews. Een overzicht van het interview ziet men in tabel 23. Dit is een interview geweest met de C.T.O. van het bedrijf; Camiel Dobbelaar.

TABEL 23; INTERVIEW EISEN EN WENSEN – CAMIEL DOBBELAAR

Vraag	Antwoord/opmerking
Aan welke eisen dient de nieuwe firewall te voldoen?	Na overleg met Camiel Dobbelaar is de student samen met Camiel op een aantal eisen/wensen gekomen; de eisen/wensen zijn als volgt; *Performance, High Availability, Beheerbaarheid, Automatisering, IPv6 Routering, VXLAN, Open-Source, Distributed firewall en Quality* en *Service*
Wat is een goede test om de functionaliteit van de nieuwe firewall te testen?	Met het programma 'iPerf' kunnen er TCP-sessies worden opgezet. Het programma kan verschillende parallelle sessies opzetten, hierdoor kan de bandbreedte maximaal getest worden.
Wat dient er geautomatiseerd te kunnen worden?	De firewall rules moeten via een script automatisch ingevoerd kunnen worden. De beheerder hoeft dus niet op de firewall zelf in te loggen om rules aan te maken, dit dient automatisch te kunnen.
Wat wordt er verstaan onder beheerbaarheid?	De firewall dient een gebruikersinterface (GUi) te hebben dat het netwerk overzichtelijk maakt. Ook dient de firewall beheerbaar te zijn zonder een gebruikersinterface waardoor automatisering mogelijk wordt.

Eisen en wensen

In deze paragraaf zullen de eisen en wensen worden uitgelegd en er zal duidelijk worden gemaakt waarvoor de eisen en wensen dienen.

Performance/Multi-CPU

In de huidige situatie presteert de firewall niet naar behoren. Er worden te veel resources (CPU verbruik) gebruikt bij het aanzetten van de 'fail-over'. Het toevoegen van meerdere virtuele CPU's heeft geen baat omdat het huidige besturingssysteem hier niet goed mee om gaat. Het nieuwe pakket dient compatibel te zijn met meerdere virtuele CPU's en dient maximaal voor 70% belast te kunnen worden bij intensieve routeringen/taken.

High Availability

Het uiteindelijke pakket dient bij uitval van de firewall alle verbindingen naar een back-up firewall te sturen. De verbindingen dienen met behoud van de sessie informatie overgezet te worden. Dit houdt in dat alle verbindingen hun informatie behouden en niet verbroken worden als de back-up firewall wordt ingezet bij een fail-over.

Beheerbaarheid/Automatisering

Omdat beheerbaarheid een belangrijk onderwerp is dient de nieuwe firewall op verschillende manieren beheerd te kunnen worden. Zo moet het nieuwe pakket een web-interface hebben waarin er een visueel overzicht is van het netwerk en moet het pakket te automatiseren zijn. Dit houdt in dat er via scripts/commando's verschillende firewall regels aangepast kunnen worden en dat het pakket te beheren is zonder gebruik te maken van de web-interface.

Monitoring

Omdat het nieuwe pakket zorgt voor de beveiliging en het aanbieden van services (gateway/load-balacing/fail-over/DNS) voor de klant omgeving, dient het pakket zorgvuldig gemonitord te worden. Dit kan gedaan worden door het pakket op te nemen in de huidige monitoring van het bedrijf. Hierdoor kunnen de verschillende netwerken en services gemonitord worden. Meer hierover kan men vinden in het hoofdstuk '*Monitoring*'.

IPv6 Routering

Omdat de IPv4 nummering langzamerhand op raakt is het de wens dat het nieuwe pakket compatibel is met IPv6. IPv6 is de opvolger van IPv4 en in een 'dual-stack' mode kan het pakket met beide protocollen omgaan.

VXLAN

VXLAN is de opvolger van het VLAN-protocol. Met het VLAN-protocol kunnen er maximaal 4096 netwerken worden gemaakt. Omdat dit limiet tegenwoordig met Cloud-computing gemakkelijker behaald kan worden is het de wens dat het nieuwe pakket het VXLAN-protocol ondersteunt. Met het VXLAN-protocol kunnen er ongeveer 16.000.000 (16 miljoen) netwerken gecreëerd worden.

Open-source

Omdat het bedrijf veel met open source producten werken, heeft het bedrijf de wens dat de firewall ook open source is. Dit is niet noodzakelijk, vandaar dat dit als wens genoteerd is. Mocht er een betaald pakket zijn die beter aan de eisen en wensen van het bedrijf voldoet, dan mag dit pakket geadviseerd worden.

Distributed firewall

Om de beveiliging van de services zo veilig mogelijk te houden is het de wens dat de gedistribueerde firewall beveiligingen toe kan voegen op VM-niveau. Op de traditionele manier worden de beveiligingen op het netwerkniveau gedaan. Het is de wens van het bedrijf om een extra laag beveiliging toe te voegen. Dit stelt het in staat om binnen een netwerk beveiligingen toe te passen op server/VM-niveau.

Quality of Service

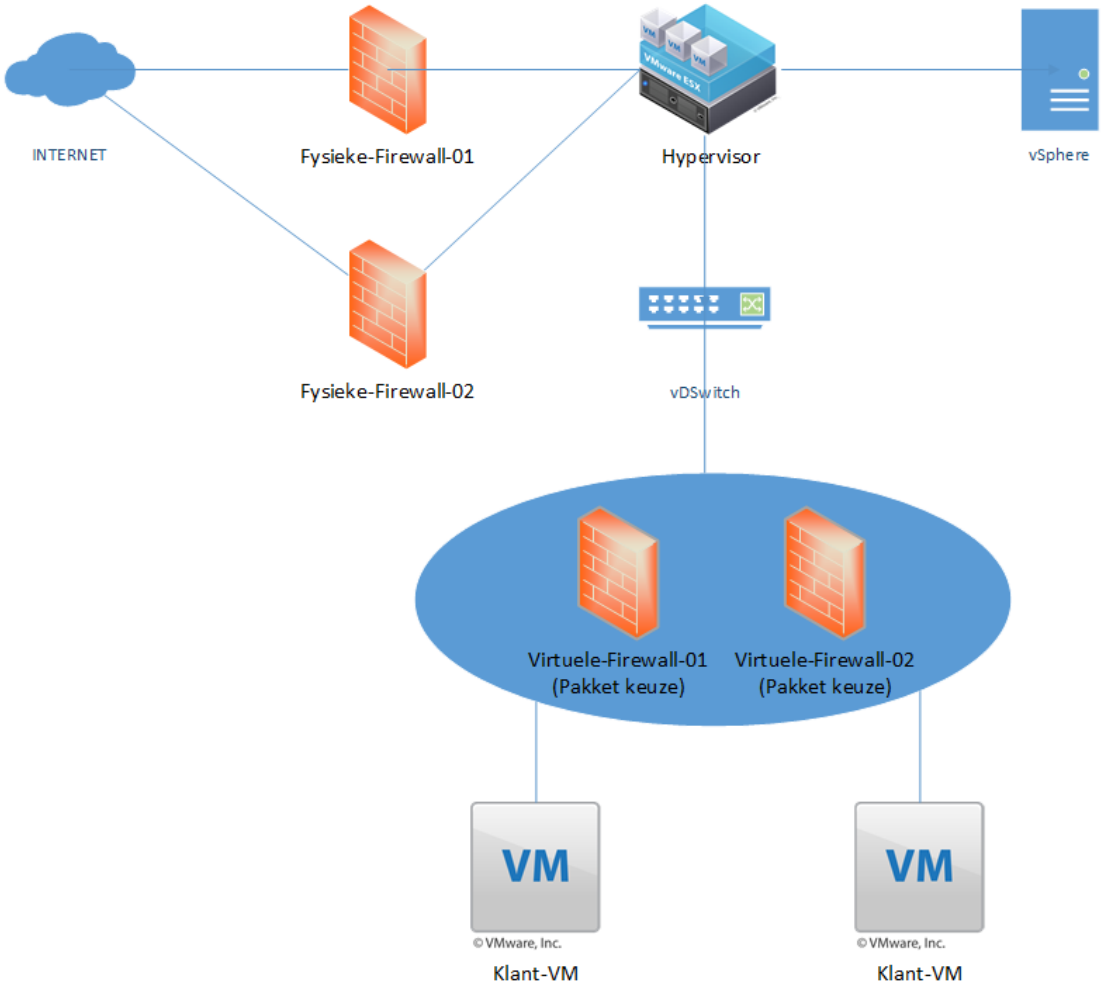
Om bepaald verkeer voorrang te geven is het de wens dat de nieuwe firewall pakketten kan prioriteren, zodat er voorrang verleend kan worden aan een bepaalde verkeersstroom. Dit is als wens genoteerd, dus het is niet noodzakelijk dat het nieuwe pakket aan dit protocol moet voldoen.

Architectuur

In dit hoofdstuk zal de architectuur van het ontwerp dat ontworpen zal worden, worden beschreven. Het ontwerp moet het in staat stellen om aan de eisen en wensen te voldoen die in het hoofdstuk '*Functionele eisen en wensen*' worden genoemd. De componenten die deel maken van de architectuur zullen per component apart beschreven worden.

Het doel van de architectuur is om een sjabloon te maken waarin het niet uit maakt welk pakket er gekozen wordt. De architectuur is dus pakket onafhankelijk.

Een overzicht van de architectuur bevindt zich in afbeelding 32;



AFBEELDING 32; ARCHITECTUUR

Componenten architectuur

In afbeelding 1 zijn een aantal componenten te zien die deel uitmaken van de architectuur. De componenten zijn als volgt;

- Fysieke-Firewall
- Hypervisor
- vSphere
- vDSwitch
- Virtuele-Firewall
- Klant-VM

Om een duidelijk beeld te schetsen van de architectuur zullen de componenten apart worden beschreven

Fysieke-Firewall

Dit is een fysieke machine die dient als firewall voor bescherming tegen het internet. Deze firewall dient als eerste beveiligings-laag van het netwerk en zorgt ervoor dat het verkeer gefilterd wordt zodat het netwerk beschermd wordt tegen aanvallen van buitenaf. Hierdoor is het netwerk alleen toegankelijk voor geautoriseerde medewerkers. In afbeelding 1 is de Fysieke-Firewall dubbel uitgevoegd, dit is gedaan om de load-balancing/fail-over in kaart te brengen,

Hypervisor

Een hypervisor is een fysieke machine/server waarop een licht besturingssysteem wordt geïnstalleerd. Een hypervisor stelt het in staat om op een fysieke machine, virtuele machines te creëren en te beheren. Hierdoor kunnen er meerdere machines/besturingssystemen op dezelfde fysieke machine draaien. De hypervisor heeft een geïntegreerde switch waaraan virtuele machines gekoppeld kunnen worden. Meer over de switch is te vinden in het kopje '*vDSwitch*'.

vSphere

De vSphere is een virtuele machine op de hypervisor die het in staat stelt om de hypervisor te beheren. Via de vSphere kunnen er virtuele machines gecreëerd worden en beheerd. Ook kunnen er verschillende netwerken gecreëerd worden die gekoppeld zijn met de '*vDSwitch*'. vSphere zorgt voor een centrale plek waar de virtuele omgeving te beheren is.

vDSwitch

De vDSwitch is een virtuele gedistribueerde switch die geïntegreerd is in de hypervisor. Via de vSphere kan de switch beheer worden. Zo kunnen er verschillende netwerken worden gecreëerd (VLAN's) en kunnen er per VLAN verschillende instellingen (Trunk/VLAN ID) worden aangepast. Een Virtual Distributed Switch (vDSwitch) is een switch die meerdere ESXI hosts met elkaar kan laten communiceren. Zo kunnen de VLAN's 'doorgetrokken' worden naar meerdere (fysieke) ESXI hosts en kunnen de hosts samen werken met de verschillende netwerken.

Virtuele-Firewall

De virtuele firewall zorgt voor de communicatie tussen de verschillende netwerken. Op de virtuele firewall kunnen er verschillende regels worden aangemaakt. Zo kan bijvoorbeeld netwerk-1 geblokkeerd worden vanaf netwerk-2. De virtuele firewall is het pakket waar de student onderzoek naar doet. Uit de short list is er gebleken dat er drie pakketten zijn die voldoen aan de eisen van de klant. De verschillende pakketten nemen dus de plaats in van de virtuele firewall. In afbeelding 1 is de Virtuele-Firewall (het pakket) dubbel uitgevoerd, dit is gedaan om de load-balancing/fail-over in kaart te brengen.

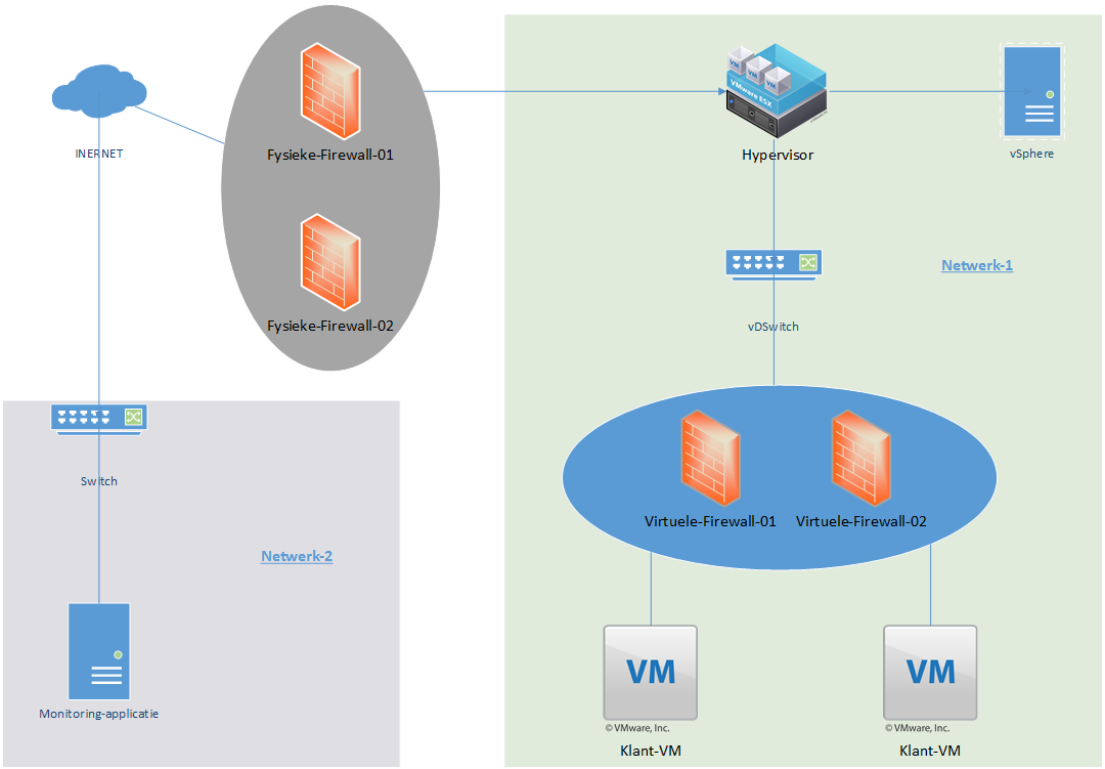
Klant-VM

Dit zijn de virtuele machines die draaien op de hypervisor. De virtuele machines kunnen diensten leveren aan de klanten van het bedrijf. Bijvoorbeeld een web/ftp/file server die vanaf het internet te benaderen is. In de tekening zijn er twee Klant-VM's geïllustreerd, in de werkelijkheid zijn dit er vele male meer, maar om te tekening overzichtelijk te houden, heeft de student er twee als voorbeeld gegeven.

Monitoring

Omdat de nieuwe virtuele firewall services levert aan klanten van het bedrijf, dient de firewall goed gemonitord te worden. De huidige virtuele firewall wordt niet gemonitord omdat hier nog geen goed monitor ontwerp voor is ontworpen. Een ontwerp voor de monitoring kan men vinden in afbeelding 2. De firewall zal niet alleen gemonitord worden op up-time (of de firewall online is of niet) maar ook op de services en verschillende netwerken die de firewall aanbiedt voor de virtuele machines.

De firewall wordt gemonitord worden via een apart netwerk, netwerk 2 in afbeelding 2. Dit wordt gedaan zodat de monitoring online blijft als het netwerk van de virtuele firewall eruit ligt. Deze manier van monitoring wordt een 'out-of-band' monitoring genoemd. Een overzicht van hoe de monitoring plaats kan vinden ziet men in afbeelding 33;



AFBEELDING 33; MONITORING

Monitoring-applicatie

De monitoring-applicatie in afbeelding 33 is aangesloten op een apart netwerk. Via dit netwerk (netwerk-2) is het netwerk van de virtuele firewall (netwerk-1) benaderbaar voor monitoring. De monitoring wordt gebruikt om verschillende services te monitoren. Om dit in staat te stellen kan er gebruik gemaakt worden van het SNMP-protocol. SNMP staat voor 'Simple Network Management Protocol'.

Via dit protocol kunnen de services worden gemonitord. Zo kan er gemonitord worden op services, zoals SSH, maar ook op netwerkniveau. Dit houdt in dat de verschillende netwerken op de virtuele firewall ook gemonitord kunnen worden. Als er verschillende netwerken aanwezig zijn (VLAN's/VXLAN's) dan wordt er gemonitord op de interface van het betreffende netwerk.

Bijlage - Beheerplan

Inleiding

Dit document is opgesteld door de student om het beheer van het nieuwe pakket in kaart te brengen. Het beheer van het nieuwe pakket dient op minimaal twee verschillende manier gedaan te kunnen worden. Beheer is een belangrijk punt voor het bedrijf en in dit document zullen de verschillende manier van het beheer worden beschreven.

Doelstelling

De doelstelling van dit document is om het beheer in kaart te brengen. Er zullen verschillende manieren van beheer worden uitgelegd en er zal duidelijk worden gemaakt welke manier van beheer voor welk doeleinde dient.

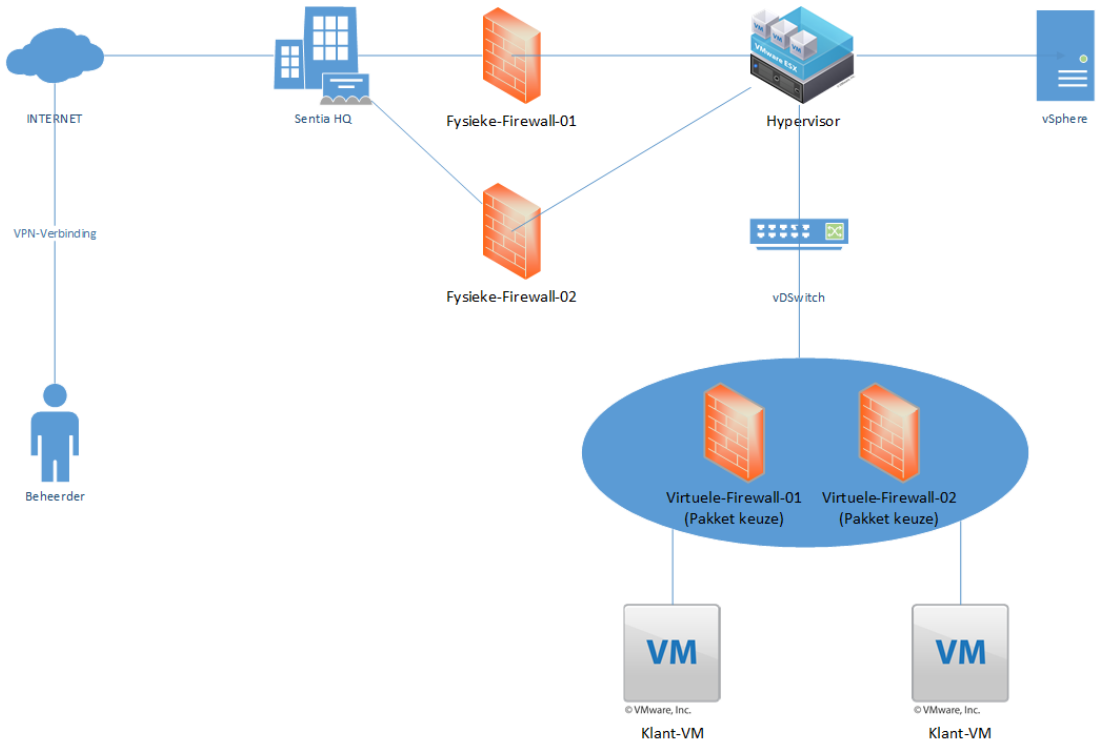
Eisen

Het beheer dient aan een aantal eisen te voldoen. De eisen waaraan het beheer moet voldoen zijn als volgt;

- Beheer via de interface van het pakket; Hierdoor is er een visueel overzicht mogelijk van het netwerk.
- Beheer via automatisering; Het beheer moet geautomatiseerd worden, hierdoor is het mogelijk om verschillende aanpassingen te doen aan het pakket zonder in te loggen om de (web)interface van het pakket. Aanpassingen dienen via bijvoorbeeld een script doorgevoerd kunnen worden.
- Het pakket dient een overzicht te hebben van alle netwerken en, indien er ingelogd wordt met het ‘administrator’ account, dienen alle netwerken beheerd te kunnen worden.
- Het pakket dient beheerbaar te zijn voor verschillende netwerken. Dit houdt in dat er bijvoorbeeld beheer gedaan kan worden voor een apart netwerk op de firewall. Als bijvoorbeeld netwerk A en B zijn aangemaakt op de firewall, dan dienen de firewall instelling voor netwerk A en netwerk B afzonderlijk van elkaar beheerd te kunnen worden. Op deze manier wordt het mogelijk gemaakt dat de beheerder van netwerk A, niet bij de firewall van netwerk B kan.

Overzicht beheer

In deze paragraaf zal het overzicht van het beheer worden geschetst. Voor het overzicht wordt men verwezen naar afbeelding 34;



AFBEELDING 34; BEHEER PAKKET

De beheerder logt via een VPN-verbinding via het internet in op een van de kantoren van het bedrijf. Als de beheerder eenmaal ingelogd is, dan kan de beheerder via de VPN het pakket managen.

Beveiliging

Omdat het niet mogelijk mag zijn dat iedereen bij het beheer van het nieuwe pakket kan moet dit beveiligd worden. Dit kan gedaan worden door middel van het opzetten van een VPN-connectie naar het managementnetwerk. Vanuit het managementnetwerk is er een verbinding mogelijk naar de beheerinterface van het pakket.

Alleen geautoriseerde medewerkers kunnen inloggen op de VPN. Om hier in aanmerking voor te komen dient dit overlegd te worden met de teamleider. Medewerkers die geautoriseerd zijn kunnen inloggen met een gebruikersnaam, wachtwoord en een bijbehorend certificaat. Op de manier kan er met grote zekerheid wordt gezegd dat alleen medewerkers die toegang hebben tot de VPN, daadwerkelijk zijn ingelogd.

Bijlage 5: Technisch Ontwerp

Technisch Ontwerp

Sentia B.V.

Vak-code: Afstuderen (TICT-AFSTUD-12)

Klas: SV3A

Versie: 1.0

Datum: 14-1-2016

R. Badal 1607426 ricky.badal@student.hu.nl

Technisch Ontwerp, Utrecht, 14-1-2016

R. Badal

Versiebeheer

Hieronder volgt het versiebeheer.

Versie	Datum	Opmerkingen
0.1	22-12-2015	Origineel document opgesteld.
0.2	14-01-2016	Technische ontwerpen toegevoegd.
0.3	05-02-2016	Commentaar Jos verwerkt.

Inhoudsopgave

Inleiding

In dit document zal het Technisch Ontwerp voor de afstudeeropdracht van de student worden beschreven. Tijdens de onderzoeksfase heeft de student een aantal eisen en wensen in kaart gebracht waaraan het eindproduct moet voldoen, deze eisen en wensen kan men terug vinden in het Functioneel Ontwerp. Dit document zal de technische functies beschrijven die het uiteindelijke pakket zal moeten hebben om aan de wensen en eisen van het bedrijf te voldoen en is een vervolg op de functionele eisen van het Functioneel Ontwerp.

De opdracht die de student zal moeten uitvoeren kan omschreven worden als een ontwerp/advies opdracht. Om de afstudeeropdracht structuur te geven is de opdracht verdeeld in verschillende fases. Het Technisch Ontwerp is onderdeel van de afstudeeropdracht en maakt deel uit van de *Ontwerpfase*.

De technische specificaties van de functies waaraan het pakket zal moeten voldoen zullen in dit document worden beschreven.

Doelstelling

De doelstelling van dit document is om de technische specificaties te leveren bij de functionele eisen en wensen waaraan het uiteindelijke pakket aan zal moeten voldoen. In dit document zullen de pakketten uit de ‘short-list’, van het onderzoeksrapport, worden beschreven en de technische aspecten van de pakketten zullen per pakket worden gedocumenteerd. De pakketten die in dit document beschreven zullen worden zijn;

- pfSense
- VMWare NSX
- Contrail

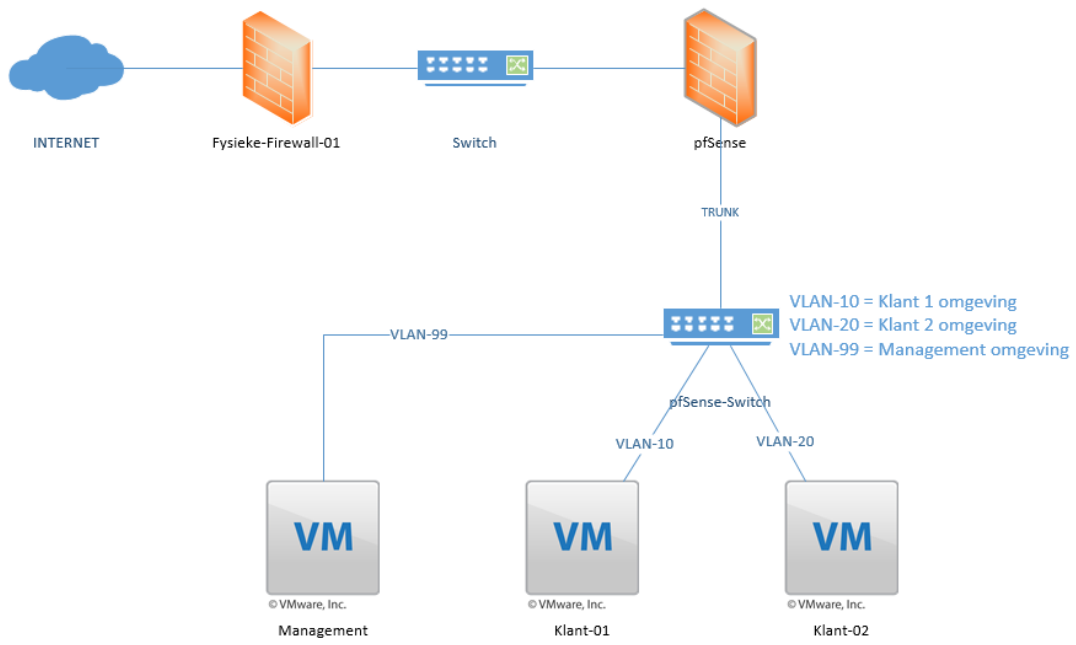
Aan de hand van dit document kan een technische medewerker van het bedrijf de proefopstelling van de student nabouwen en kunnen de technische specificaties worden overgenomen om zo de verschillende pakketten te integreren in de huidige infrastructuur.

Technisch Ontwerp

In dit hoofdstuk zal het technisch ontwerp worden beschreven. Het ontwerp is gemaakt om zo de verschillende componenten in kaart te brengen. De verschillende technische componenten zullen per component worden beschreven in dit document en er zal duidelijk worden gemaakt waarvoor de componenten dienen en wat de technische specificaties hiervan zijn. Omdat de shortlist bestaat uit drie pakketten, zullen er drie technische ontwerpen worden gemaakt.

pfSense

In deze paragraaf zal het technisch ontwerp van het pakket '*pfSense'* worden beschreven. De technische specificaties van het ontwerp zullen in deze paragraaf worden gedocumenteerd. Een Layer-2 overzicht van het technisch ontwerp kan men vinden in afbeelding 35;



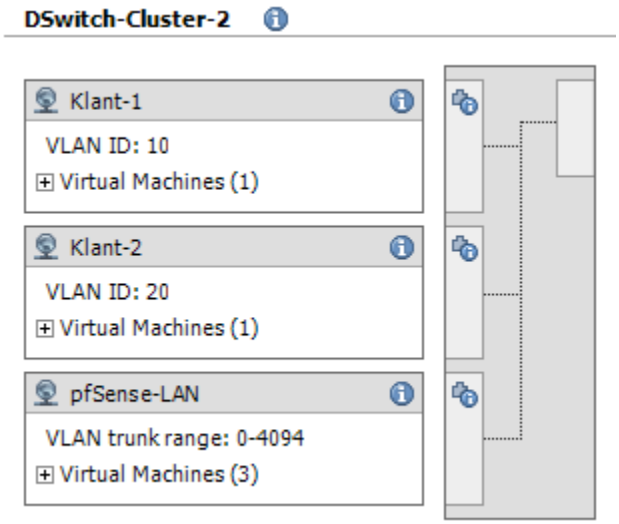
AFBEELDING 35; TECHNISCH ONTWERP PFSENSE

Fysieke firewall

De *fysieke firewall* heeft een verbinding met *pfSense* via het 172.16.0.0/24 netwerk. Voor pfSense is dit de toegang naar het internet. *Pfsense* routeert al het verkeer dat naar buiten wilt naar de fysieke firewall, die het verkeer vervolgens weer naar het internet routeert.

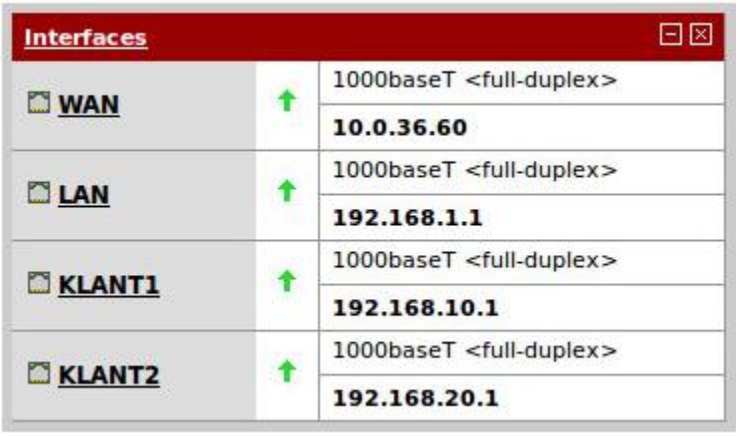
vCenter/vDSWitch

Via de *vCenter* kan de hypervisor beheerd worden. Als er eenmaal ingelogd is dan kunnen de VLAN's worden aangemaakt op de *vDSwitch*. Hieronder in afbeelding 36 ziet men een overzicht van de aangemaakte VLANs op de *vDSwitch*;



AFBEELDING 36; VLAN'S PFSENSE

De VLAN ID's worden doorgestuurd naar *pfSense* en op pfSense worden de bijbehorende gateways aangemaakt met het bijbehorende VLAN ID. Een overzicht van de gateways die aangemaakt zijn en de VLAN ID's vindt men in afbeelding 37;



AFBEELDING 37; GATEWAYS PFSENSE

Management-VM

De *Management* VM is een virtuele machine die gebruikt wordt om *pfSense* te beheren. De LAN-interface van *pfSense* zit in hetzelfde netwerk als de *Management* machine.

Klant-VM

De IP-instellingen van de Klant-01 zijn in tabel 24 te vinden:

TABEL 24; KLANT-01 IP SETTINGS

Klant-01 machine	
IP-adres	192.168.10.10
Subnet	255.255.255.0
Gateway	192.168.10.1

De gateway is ingesteld op *pfSense* en zorgt onder andere voor communicatie met de buitenwereld en de *Klant-02* machine.

De IP-instellingen van de Klant-02 machine zijn in tabel 25 te vinden:

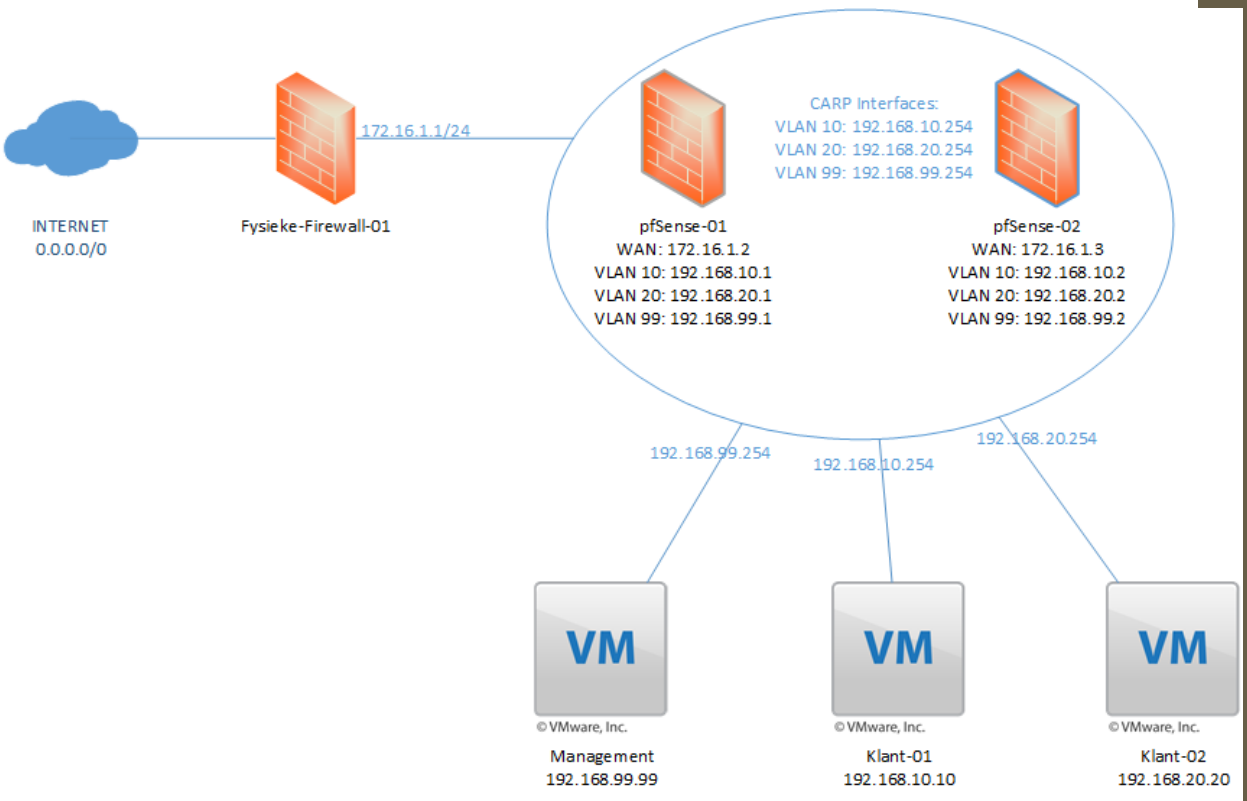
TABEL 25; KLANT-02 IP SETTINGS

Klant-02 machine	
IP-adres	192.168.20.20
Subnet	255.255.255.0
Gateway	192.168.20.1

De gateway is ingesteld op *pfSense* en zorgt onder andere voor communicatie met de buitenwereld en andere klant machines.

Logische netwerktekening

Om een beter overzicht te krijgen van het netwerk is er een logische netwerktekening gemaakt op laag-3 niveau. In dit overzicht ziet men de IP-adressen en interfaces die verbonden zijn met het bijbehorende subnet. Een overzicht van de tekening kan men vinden in afbeelding 38;



AFBEELDING 38; LOGISCH OVERZICHT PFSENSE

CARP-Interfaces

Om High Availability te configureren, wordt er gebruik gemaakt van het CARP-protocol. Het CARP-protocol stelt het in staat om bij uitval van *pfsense-01* de verbindingen over te laten nemen door *pfsense-02*. Op deze manier kunnen klanten verder werken als er een firewall uitvalt. De klanten VM's hebben als gateway virtuele IP-adressen, deze worden door middel van het CARP-protocol virtueel aangeboden. Een overzicht van de CARP IP-adressen vindt men in afbeelding 39;

Status: CARP

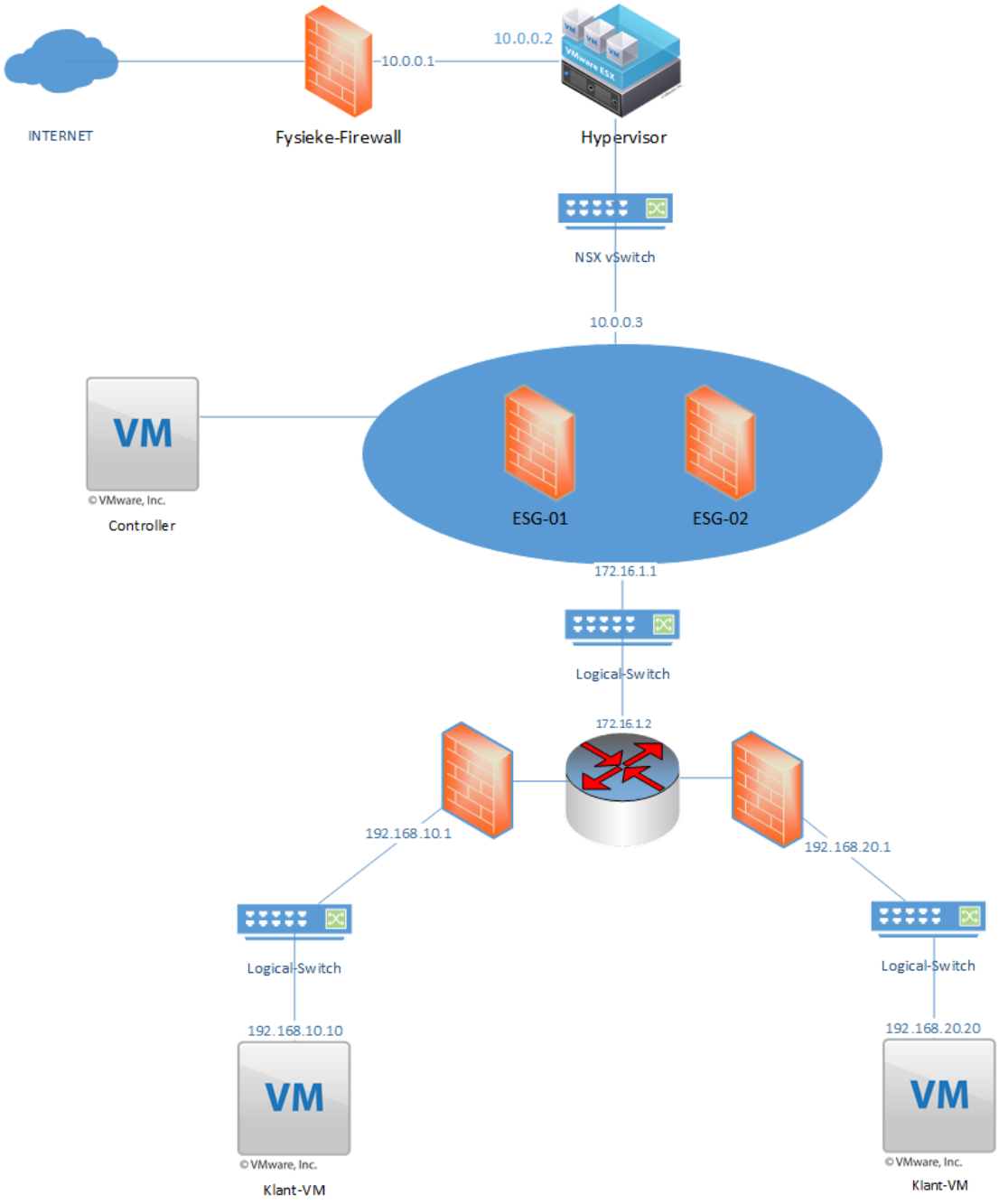
Temporarily Disable CARP | Enter Persistent CARP Maintenance Mode

CARP Interface	Virtual IP	Status
KLANT1@1	192.168.10.254	MASTER
KLANT2@2	192.168.20.254	MASTER

AFBEELDING 39; VIRTUELE IP ADRESSEN

VMware NSX

In deze paragraaf zal het technisch ontwerp van het pakket '*VMware NSX'* worden beschreven. De technische specificaties van het ontwerp zullen in deze paragraaf worden gedocumenteerd. Een overzicht van het technisch ontwerp kan men vinden in afbeelding 40;



AFBEELDING 40; VMWARE NSX ONTWERP

Logische switches

VMWare NSX maakt gebruikt van logische switches. Logische switches simuleren fysieke switches in een virtuele omgeving. Zo kan elke VM op een andere logische switch worden aangesloten. De VM's kunnen ook op dezelfde logische switch aangesloten worden. De VM's onderling kunnen via het VXLAN-protocol met elkaar communiceren. Elke logische switch krijgt een segment ID (net als een VLAN ID). Er kunnen ongeveer 16 miljoen segment ID's aangemaakt worden. Een overzicht van de logische switches ziet men in afbeelding 41;

Name	Status	Transport Zone	Scope	Segment ID	Control Plane Mode
klant-1-switch	Normal	Transport-Zone	Global	5000	Unicast
klant-2-switch	Normal	Transport-Zone	Global	5001	Unicast
transit	Normal	Transport-Zone	Global	5002	Unicast

AFBEELDING 41; LOGISCHE SWITCHES NSX

Controller

De controller wordt gebruikt om de firewalls te beheren. Via de controller is centraal beheer mogelijk. De controller heeft alle informatie over de logische switches, virtuele machines, ESXi hosten en VXLAN's. Op deze manier kunnen de verschillende firewalls voor de verschillende netwerken worden aangesproken. In de testomgeving zijn er drie controller gecreëerd om zo High Availability omhoog te houden. In afbeelding 42 ziet men een voorbeeld van de controllers;

NSX Controller nodes

Actions

Controller IP Address	ID	Status	Software Version
10.0.36.43	controller-12	Normal	6.2.44780
10.0.36.44	controller-13	Normal	6.2.44780
10.0.36.45	controller-14	Normal	6.2.44780

AFBEELDING 42; NSX CONTROLLERS

Edge Service Gateway

De ESG zorgt voor de verbindingen die naar buiten gaan en van buiten komen. Op de ESG kunnen aparte firewall rules worden gemaakt voor verbindingen van en naar het internet. Deze firewall rules worden toegepast op de VM's voor de verbindingen van en naar buiten. Om firewall rules te maken die alleen gelden voor communicatie tussen de VM's kunnen er firewall rules gemaakt worden op de DLR. In afbeelding 43 kan men zien hoe de routering plaats vindt op de ESG en ziet men dat middels het OSPF-protocol de routes worden gedeeld;

```
S        0.0.0.0/0              [0/0]          via 10.0.36.1
C        10.0.36.0/24           [0/0]          via 10.0.36.55
C        172.16.1.0/24          [0/0]          via 172.16.1.1
O   E2   192.168.10.0/24        [110/1]        via 172.16.1.2
O   E2   192.168.20.0/24        [110/1]        via 172.16.1.2
```

AFBEELDING 43; ROUTING TABEL ESG

Op de ESG zijn er twee interfaces aangemaakt. Een interface voor de connectie naar de buitenwereld, en een interface voor de communicatie tussen de DLR en de ESG. In afbeelding 44 ziet men de interfaces die aangemaakt zijn op de ESG;

Configure interfaces of this NSX Edge.

Actions

Filter

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To	Type	Status
0	uplink	10.0.36.60*	24	VDS-NSX-MAN	Uplink	✔
1	to-DLR	172.16.1.1*	24	transit	Internal	✔

AFBEELDING 44; INTERFACES ESG

Distributed Logical Router

De DLR zorgt voor de communicatie tussen de VM's. De verbindingen naar buiten worden beheerd door de ESG. Op de DLR kunnen firewall rules aangemaakt worden die het verkeer van en naar de verschillende VM-netwerken regelt. De DLR regelt dus alleen het verkeer van de interne VM-netwerken. In afbeelding 45 kan men zien hoe de routering plaats vinden op de DLR;

```
S        0.0.0.0/0              [0/0]          via 172.16.1.1
O   E2   10.0.36.0/24           [110/0]        via 172.16.1.1
C        169.254.1.4/30         [0/0]          via 169.254.1.5
C        172.16.1.0/24          [0/0]          via 172.16.1.3
C        192.168.10.0/24        [0/0]          via 192.168.10.1
C        192.168.20.0/24        [0/0]          via 192.168.20.1
DLR-0> _
```

AFBEELDING 45; ROUTING TABEL DLR

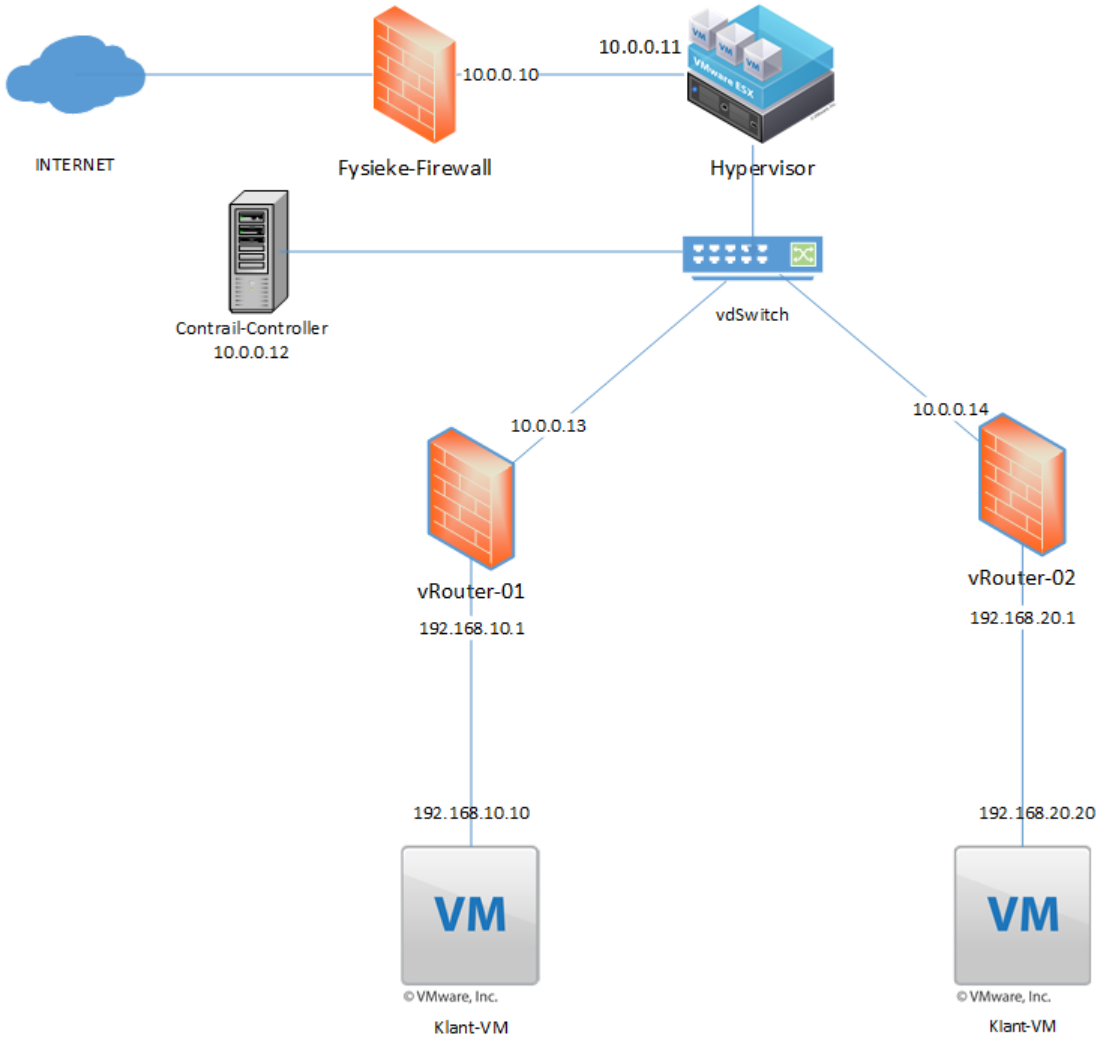
Op de DLR zijn er drie interfaces aangemaakt. Twee interfaces voor de twee verschillende netwerken en een interface voor de verbinding naar de ESG. In afbeelding 45 kan men zien dat er middels het OSPF-protocol routes worden uitgedeeld. In afbeelding 46 ziet men de interfaces die er aangemaakt zijn op de DLR;

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To	Type	Status
2	klant1	192.168.10.1*	24	klant1-switch	Uplink	✔
3	klant2	192.168.20.1*	24	klant2-switch	Uplink	✔
4	to-ESG	172.16.1.2*	24	transit	Uplink	✔

AFBEELDING 46; DLR INTERFACES

Contrail

In deze paragraaf zal het technisch ontwerp van het pakket '*Contrail*' worden beschreven. De technische specificaties van het ontwerp zullen in deze paragraaf worden gedocumenteerd. Een overzicht van het technisch ontwerp kan men vinden in afbeelding 47;



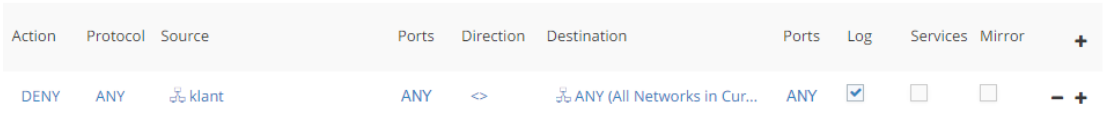
AFBEELDING 47; CONTRAIL NETWERK

Controller

De Contrail Controller wordt gebruikt als het centrale managementsysteem. De controller heeft informatie over alle netwerken die er gecreëerd zijn en alle routers. Via de controller kunnen de routers worden aangesproken en kunnen er nieuwe netwerken worden gecreëerd en nieuwe routers worden aangemaakt.

vRouter

De vRouter heeft de informatie over de netwerken die er aangemaakt zijn. Per vRouter kunnen er verschillende netwerken worden gecreëerd. De netwerken kunnen gescheiden worden door middel van policies. In afbeelding 48 ziet men een voorbeeld van de policy die de netwerken scheidt;



AFBEELDING 48; CONTRAIL POLICY

Men ziet in afbeelding 14 dat het klant netwerken geblokkeerd wordt naar het netwerk ‘ANY’. Dit betekend dat er geen communicatie mogelijk is van het klant netwerk naar buiten/een ander netwerk en andersom.

Bijlage 6: Testplan

Testplan

Sentia B.V.

Vak-code: Afstuderen (TICT-AFSTUD-12)

Klas: SV3A

Versie: 1.0

Datum: 14-1-2016

R. Badal 1607426 ricky.badal@student.hu.nl

Testplan, Utrecht, 14-1-2016

R. Badal

Versiebeheer

Hieronder volgt het versiebeheer.

Versie	Datum	Opmerkingen
0.1	9-2-2016	Origineel document opgesteld.
0.2	15-2-2016	Feedback Jos verwerkt.
0.3	23-2-2016	Vermeld waarop de pakketten getest zullen worden.

Inhoudsopgave

Inleiding

In dit document zal er worden beschreven hoe de geadviseerde pakketten getest zullen worden. De pakketten zullen op dezelfde manier worden getest. De pakketten zullen getest worden op CPU-performance bij een routering van 1 GB/per seconden. De pakketanalyse wordt uitgevoerd met het programma ‘iPerf’. IPerf is een programma dat het in staat stelt om de maximale bandbreedte te benutten van een (virtuele)machine.

Omdat de gekozen pakketten firewalls betreffen wordt routing ook ondersteund. De manier van testen gebeurt door twee machines in verschillende netwerken met elkaar te laten communiceren middels het programma iPerf. De firewall (het geadviseerde pakket) zorgt dan voor de routering en de performance van het betreffende pakket kan dan worden gemonitord om te kijken hoe het pakket presteert onder deze omstandigheden.

Doelstelling

De doelstelling van dit document is om te achterhalen hoe de geadviseerde pakketten reageren op de testsituatie. De geadviseerde pakketten die getest zullen worden zijn;

- pfSense
- VMWare NSX
- Contrail

De pakketten zullen allemaal in dezelfde testomgeving worden getest en de testen zullen identiek aan elkaar zijn om zo gelijkmatige testresultaten te krijgen en een goede indruk te krijgen hoe het pakket presteert onder de testomstandigheden. Tijdens het Proof of Concept zullen de functionele eisen en wensen, zie hoofdstuk Eisen en Wensen in het document Functioneel Ontwerp, getoond worden aan de bedrijfsbegeleider.

Testomgeving

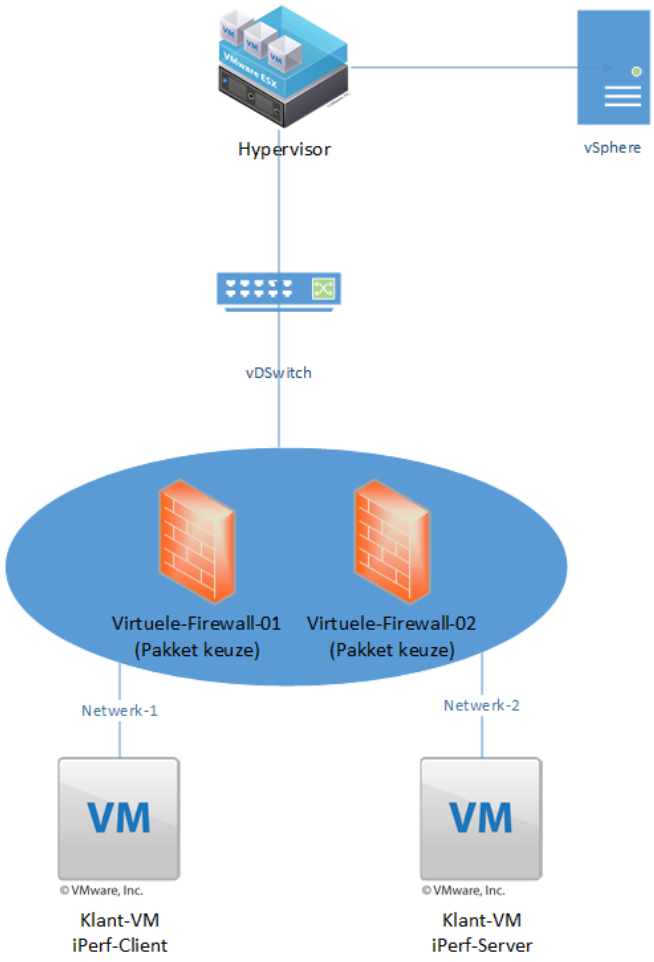
Omdat het onderzoek en het testen niet in een productie omgeving plaats kan vinden heeft de student een testopstelling gecreëerd. De testopstelling bestaat uit een fysieke machine. Deze machine simuleert de VMware ESXi 5.5 omgeving waarop de omgeving van de klanten draait.

Om de testresultaten zo veel mogelijk hetzelfde te houden als in de productie omgeving heeft de student ervoor gekozen om de productie omgeving na te bouwen als een testomgeving. De VMWare ESXi 5.5 machine is de hypervisor. Hierop draait dezelfde software als in de productie omgeving.

Op deze manier kan de student het netwerk ongeveer hetzelfde houden en worden de testresultaten niet beïnvloed door een software conflict.

Op de VMWare ESXi 5.5 machine draaien 2 virtuele machines. Deze virtuele machines staan elk apart in een ander netwerk (dit simuleert de verschillende klant omgevingen).

Het is aan de student om te onderzoeken welke virtuele firewall er het best presteert in een virtuele omgeving en welke type virtuele firewall het best in de bestaande infrastructuur past. Hieronder, in afbeelding 49, ziet men een netwerktekening van de testomgeving die de student gecreëerd heeft;



AFBEELDING 49; TESTOMGEVING

Bijlage 7: Proof of Concept

Proof of Concept

Sentia B.V.

Vak-code: Afstuderen (TICT-AFSTUD-12)

Klas: SV3A

Versie: 1.0

Datum: 14-1-2016

R. Badal 1607426 ricky.badal@student.hu.nl

Proof of Concept, Utrecht, 14-1-2016

R. Badal

Versiebeheer

Hieronder volgt het versiebeheer.

Versie	Datum	Opmerkingen
0.1	9-2-2016	Origineel document opgesteld.
0.2	13-02-2016	Feedback Jos verwerkt.

Inhoudsopgave

Inleiding

In dit document zullen de verslaggevingen van het Proof of Concept worden gedocumenteerd. De pakketten zijn getest qua functionaliteit op de performance die het pakket levert bij een routering van 1 GB/ps. Er is gekeken hoe de pakketten reageren op de geschetste situatie en de bevindingen zijn gedocumenteerd in dit document.

Doelstelling

De doelstelling van dit document is om de testresultaten die uit het Proof of Concept gekomen zijn te documenteren en zo een vergelijking te kunnen maken tussen de geadviseerde pakketten. De pakketten die getest zullen worden zijn;

- pfSense
- VMWare NSX
- Contrail

Proof of Concept

In dit hoofdstuk zullen de testresultaten komen van de pakketten die er geselecteerd zijn in de shortlist.

pfSense

pfSense is een open-source pakket dat veel firewall functies biedt. pfSense is gebaseerd op het operating-system FreeBSD en het pakket biedt statefull firewall services aan. Op de firewall functies na zijn er verschillende pakketten te installeren in pfSense waardoor de functies uitgebreid kunnen worden.

Om pfSense 'High Availible' te maken maakt pfSense gebruikt van het CARP-protocol. Er kunnen twee (virtuele) machines worden geïnstalleerd met pfSense. De eerste machine is de 'master' en de tweede machine is de 'slave'. Op beide machines moeten dezelfde netwerken bekend zijn, anders kan er geen fail-over plaats vinden. Als de 'master' firewall uitvalt, dan wordt dit opgemerkt door de 'slave' firewall en worden alle firewall functies overgeplaatst naar de 'slave' server en neemt de 'slave' server de firewall taken over. Als de 'master' firewall weer online is, dan worden de taken weer terug verplaatst naar de hoofd firewall.

Om pfSense te installeren zijn de volgende hardware specificaties nodig, deze kan men vinden in tabel 26;

TABEL 26; HARDWARE EISEN PFSENSE

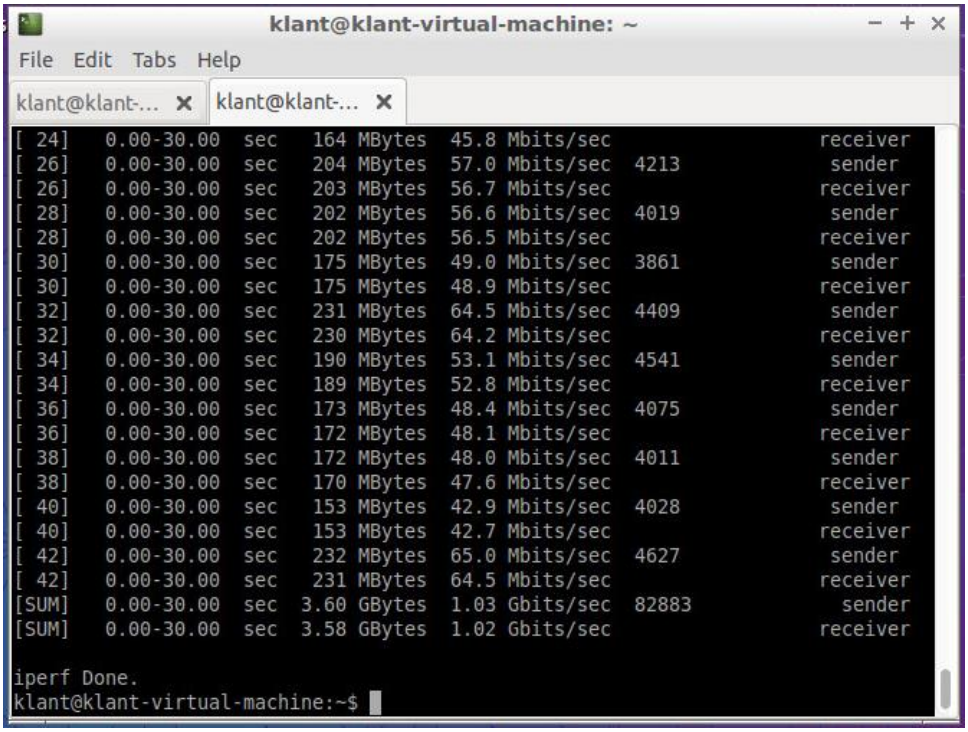
Hardware	Minimale vereiste
RAM	256 MB
Harde schijf	1 GB
CPU	500 MhZ Dual-core
Ethernet	2 ethernet poorten

Zoals er in tabel 2 te zien is heeft pfSense geen zware hardware nodig om geïnstalleerd te worden. Om dit pakket zo goed mogelijk te testen heeft de student dit pakket geïnstalleerd in de testomgeving.

Om de huidige situatie te schetsen heeft de student het pakket geïnstalleerd met een enkele CPU (zoals dit ook in de huidige situatie is).

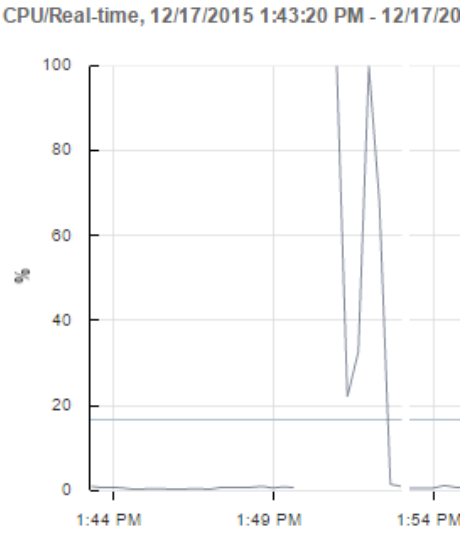
Om de performance van het pakket optimaal te testen wordt er gebruik gemaakt van het programma 'iPerf'.

In afbeelding 50 ziet men een test die gedaan is tussen twee virtuele machines in twee verschillende netwerken. Om communicatie mogelijk te maken tussen de netwerken wordt er gebruik gemaakt van de interne routing functie van het pakket.



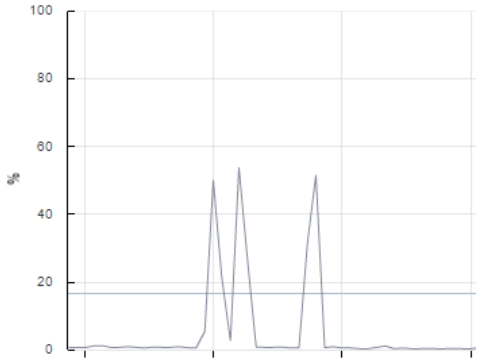
AFBEELDING 50; IPERF PFSENSE

Zoals er te zien is in afbeelding 1 wordt er een maximale bandbreedte van 1,03 Gbit per seconde gehaald. Tijdens de test is het CPU verbruik (met een enkele CPU) gemonitord. De resultaten hiervan kan men vinden in afbeelding 51;



AFBEELDING 51; 100% CPU BELASTING

In afbeelding 51 kan men zien dat de CPU van de firewall voor 100% werd verbruikt tijdens de ‘iPerf’ test. Na het toevoegen van meerdere CPU’s is de ‘iPerf’ test nogmaals gedaan, de resultaten hiervan kunt u vinden in afbeelding 52;



AFBEELDING 52; 53% CPU BELASTING

Na het toevoegen van meerdere CPU’s is het CPU verbruik bij een maximale belasting van 1 GBit / per seconden 53%.

Het operating-system van pfSense gaat dus goed om met het toekennen van meerdere CPU’s en de belasting wordt verdeeld tussen de meerdere CPU’s.

Conclusie

In de eisen en wensen die in het Functioneel Ontwerp staan is er vastgesteld dat de performance van de CPU van het pakket bij een routering van 1 GB/ps niet hoger mag zijn dan 70%. Tijdens het Proof of Concept van het pakket pfSense is er gebleken dat de CPU performance van het pakket op maximaal 53% ligt bij een routering van 1 GB/ps. Het pakket pfSense heeft de gevraagde functionaliteit dus behaald.

VMWare NSX

VMware NSX is een plug-in die geïnstalleerd kan worden op de hypervisor. NSX maakt het mogelijk om netwerken te creëren en te beheren via de Software Defined Datacenter architectuur. Dit houdt in dat netwerken te programmeren zijn via een controller en er aparte firewalls gecreëerd kunnen worden voor de verschillende netwerken.

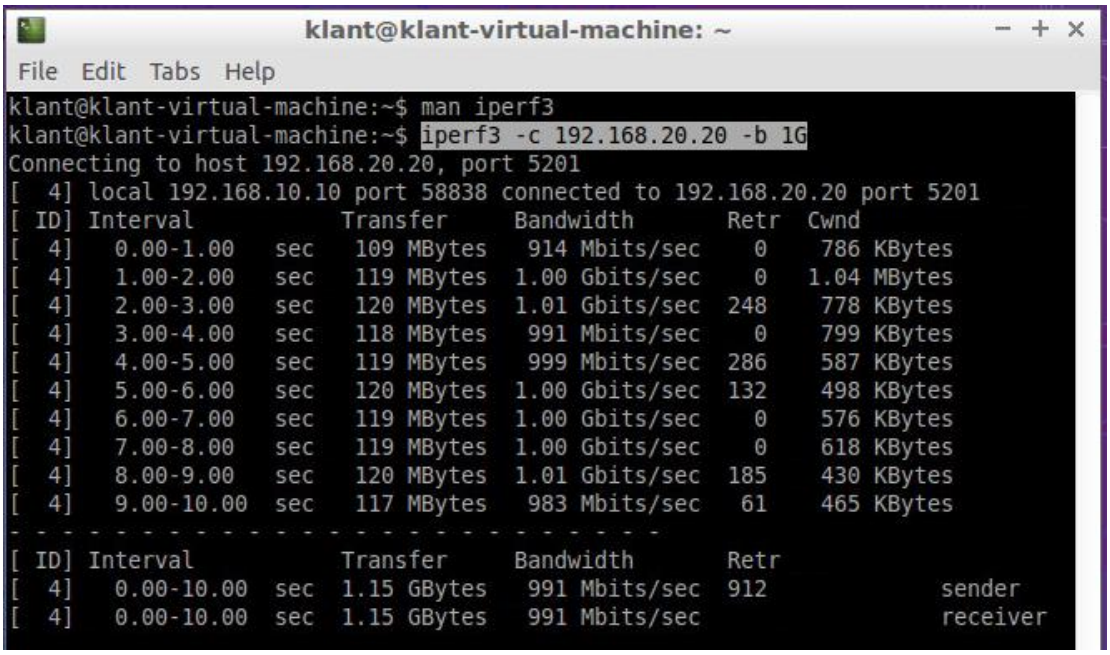
De systeemvereiste om NSX te installeren kan men vinden in tabel 26;

TABEL 26; HARDWARE EISEN NSX

Hardware	Minimale vereiste
RAM	■ NSX Manager: 12 GB ■ NSX Edge Compact: 512 MB, Large: 1 GB, X-Large: 8 GB, and Quad Large: 1 GB ■ vShield Endpoint: 1 GB ■ NSX Data Security: 512 MB
HD Ruimte	■ NSX Manager: 60 GB ■ NSX Edge Compact: 512 MB ■ vShield Endpoint: 4GB ■ NSX Data Security: 6GB per ESX host
CPU	■ NSX Manager: 4 ■ NSX Edge Compact: 1 ■ vShield Endpoint: 2 ■ NSX Data Security: 1
Ethernet	■ 1 poort

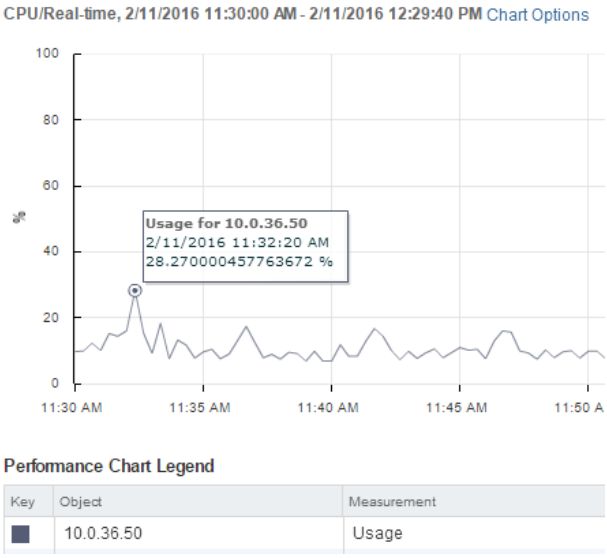
De test wordt gedaan door middel van het programma iPerf. Om ervoor te zorgen dat de firewall de routering moet voorzien wordt de communicatie geleden tussen twee verschillende machines in twee verschillende netwerken.

In afbeelding 4 is er te zien dat er verbinding wordt gemaakt met een machine in netwerk 20 (192.168.20.20). De bron machine zit in het netwerk 10 (192.168.10.10). Om de communicatie plaats te laten vinden moet er dus gerouteerd worden door de firewall en moeten de iPerf verbindingen ook gerouteerd worden. In afbeelding 53 kan men ziet dat er 1 GB/ps gerouteerd word van de ene machine naar de andere machine;



AFBEELDING 53; IPERF NSX

Omdat NSX geïntegreerd zit in de hypervisor wordt de routering niet door de firewall gedaan maar door de hypervisor zelf. Dit komt omdat de firewall de kernel van de hypervisor direct kan aanspreken en hiervoor geen eigen (virtuele) resources hoeft te gebruiken. Dit geeft als voordeel dat het weinig performance kost om de routering plaats te laten vinden, zoals men kan zin in afbeelding 54.



AFBEELDING 54; CPU VERBRUIK NSX

Zoals men zit wordt de CPU bij een routering van 1 GB/ps voor maximaal 28,27% belast. De reden dat de CPU een lage belasting heeft is omdat de firewall direct wordt aangesproken in de kernel van de hypervisor.

Conclusie

In de eisen en wensen die in het Functioneel Ontwerp staan is er vastgesteld dat de performance van de CPU van het pakket bij een routering van 1 GB/ps niet hoger mag zijn dan 70%. Tijdens het Proof of Concept van het pakket VMware NSX is er gebleken dat de CPU performance van het pakket op maximaal 28,3% ligt bij een routering van 1 GB/ps. Het pakket VMware NSX heeft de gevraagde functionaliteit dus behaald.

Contrail

Contrail is een open-source product van de fabrikant Juniper. Het pakket Contrail stelt het in staat om cloud netwerken centraal te beheren en te beveiligen. Contrail is een Cloud oplossing die door middel van SDN het in staat stelt om processen en netwerken automatisch uit te rollen. Het pakket maakt een koppeling tussen fysieke netwerken en virtuele netwerken.

Contrail bestaat uit twee versies; OpenContrail en Contrail. Qua functies zijn beide pakketten hetzelfde. Het enigste verschil is dat er bij Contrail support bijgekocht kan worden. Support wordt bij OpenContrail via de community supported. Dit betekend dat hulp meestal op forums en het internet gevonden kan worden. Contrail biedt aan bedrijven betaald support, zodat er bij calamiteiten een expert kan komen kijken wat er mis is.

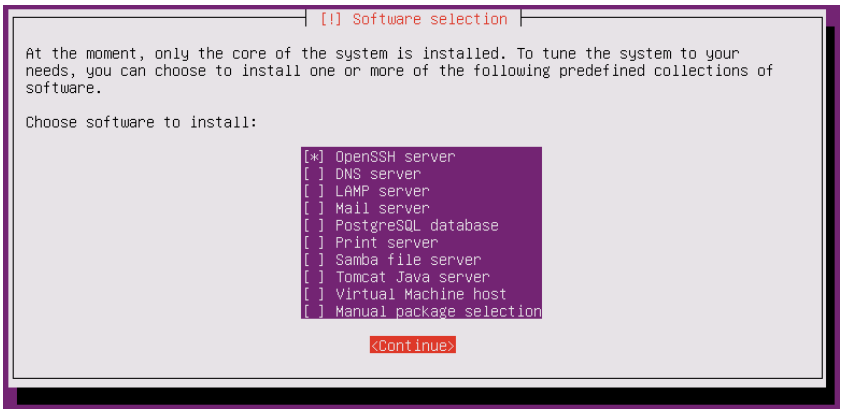
Om Contrail te implementeren zijn er een aantal minimale eisen die vereist zijn van de hardware. De hardware eisen voor Contrail kunt u vinden in tabel 27;

TABEL 27; HARDWARE EISEN CONTRAIL

Hardware	Minimale vereiste
RAM	64 GB
Harde schijf	120GB
CPU	Quad core 64 Bits
Ethernet	1 poort

Om het pakket Contrail te testen heeft de student ervoor gekozen om het pakket te installeren op een Ubuntu Server. Omdat Contrail een open-source product is, is het compatibel met vele open-source operating systems.

Voor het Proof of Concept maakt de student gebruik van Ubuntu Server versie 14.04. Tijdens de installatie moet de SSH-server worden aangevinkt zodat remote toegang mogelijk is tot de server. Zie afbeelding 55;



AFBEELDING 55; ENABLE SSH UBUNTU

Als de installatie van de server eenmaal gelukt is dan kunnen de pakketten worden gedownload op de server. Om Contail werkend te krijgen dienen de volgende pakketten gedownload te worden van de Juniper website en op de server aanwezig te zijn, zie afbeelding 56;

Ubuntu 14.04 + Juno	MD5 SHA1	2.22.0	deb	438,148,302	04 Feb 2016
Ubuntu 14.04 + vCenter	MD5 SHA1	2.22.0	deb	433,756,432	04 Feb 2016
Ubuntu 14.04 ESXi VM Host	MD5 SHA1	2.22.0	vmdk	1,063,252,480	04 Feb 2016

AFBEELDING 56; CONTRAIL PACKAGES

Nadat de software gedownload is kunnen de pakketten geïnstalleerd worden middels het volgende commando; "*dpkg –i conrail-package-ubuntu-14.04.deb"*

Als de installatie eenmaal voltooid is kunnen de utilities worden geïnstalleerd die nodig zijn voor het pakket Contrail. Deze kan men vinden in de volgende folder; "*/opt/contrail/contrail_packages".*

In deze folder bevindt zich het setup script om de gewenste software te installeren. Het script is met het volgende commando te installeren; *"./setup.sh".* Als het script succesvol uitgevoerd is ziet men het volgende bericht, zie afbeelding 57;

```
Successfully installed Fabric
Cleaning up...
root@contrail:/opt/contrail/contrail_packages#
```

AFBEELDING 57; FABRIC INSTALL UBUNTU

Nadat de juiste software geïnstalleerd is moet de kernel van het OS worden aangepast naar een versie die compatibel is met Contrail. Om de kernel versie van het OS aan te passen dient men zicht te bevinden in de folder; *"/opt/contrail/utils"* en dient met het volgende commando uit te voeren: "*fab upgrade_kernel_all".* Na het uitvoeren van dit commando zal de server opnieuw opgestart worden met de nieuwe kernel.

Omdat de huidige situatie in een VMWare ESXi 5.5 omgeving draait, dient de integratie met Contrail geconfigureerd te worden. De configuratie van de ESXi omgeving word gedaan in het bestand *"testbed.py"* in de folder *"/opt/contrail/utils/fabfile/testbed".* In afbeelding 58 ziet met de configuratie van de ESXi omgeving;

```
esxi_hosts = {
        'esxi': {
                'ip': '10.0.36.52',
                'username': 'root',
                'password': 'Welkom01',
                'datastore': "/vmfs/volumes/datastore1",
                'cluster': "Contrail-Cluster",
                   'fabric_vswitch': 'vSwitch0',
                   'fabric_port_group': 'VM Network',
                   'uplink_nic': 'vmnic0',
                'contrail_vm': {
                        'mac': "00:50:56:05:ba:ba",
                        'host': "root@10.0.36.27",
                        'vmdk': "/root/Downloads/vmdk.vmdk",
                }
        }
         }
```

AFBEELDING 58; ESXI CONTRAIL

Als de instellingen van de ESXi omgeving correct zijn overgenomen dan kan er door gegaan worden naar de volgende stap. Contrail heeft een vereiste dat er op elke ESXi host een ComputeVM wordt uitgerold. De ComputeVM zorgt voor de routering van het netwerk en op deze VM kunnen er firewall rules worden aagemaakt. Om de ComputeVM uit te rollen op de bestaande omgeving dien men zich te bevinden in de folder; *"/opt/contrail/utils"* en dient ment het volgende commando uit te voeren: *"fab prov_esxi".* Na het uitvoeren van het commando wordt het VMDK-bestand naar de ESXi server gekopieerd met de configuratie die meegegeven is in het *testbed.py* bestand. Als het commando succesvol is uitgevoerd ziet men de volgende melding, zie afbeelding 59;

```
2016-02-16 09:33:03:365367: auto_restart configured successfully for ContrailVM:ContrailVM-Datace
nter-2-10.0.36.52
2016-02-16 09:33:04:527012:
2016-02-16 09:33:04:527193: Done.
2016-02-16 09:33:04:527222: Disconnecting from 10.0.36.26... done.
2016-02-16 09:33:04:591076: root@contrail:/opt/contrail/utils#
```

AFBEELDING 59; FAB PROV_ESXI

De volgende stap is om de vCenter integratie met Contrail te configureren. Om dit te doen dient men de volgende gegevens in te vullen in het *testbed.py* bestand, zie afbeelding 60;

```
env.orchestrator = 'vcenter'
env.vcenter = {
        'server':'10.0.36.51',
        'port': '443',
        'username': 'administrator@vsphere.local',
        'password': 'Welkom01!',
        'auth': 'https',
        'datacenter': 'Datacenter-2',
        'cluster': ['Contrail-Cluster'],
        'dv_switch': { 'dv_switch_name': 'kd_dvswitch',
                     },
        'dv_port_group': { 'dv_portgroup_name': 'kd_dvportgroup',
                           'number_of_ports': '3',
                     },
}
```

AFBEELDING 60; VCENTER CONTRAIL

Nadat de gegevens juist zijn overgenomen kan men de vcenter integratie installeren door het volgende commando uit te voeren; *"fab setup_vcenter".*

De student heeft vele malen geprobeerd om de integratie met de huidige omgeving werkend te krijgen. Helaas is dit niet gelukt. Tijdens het installeren loopt het script vast op de volgende error, zie afbeelding 61;

```
2016-02-16 11:56:22:388236:     for device_list in vm.config.hardware.device:
2016-02-16 11:56:22:388387: AttributeError: 'NoneType' object has no attribute '
config'
2016-02-16 11:56:22:388511: Disconnecting from 10.0.36.26... done.
2016-02-16 11:56:22:409363: Disconnecting from 10.0.36.52... done.
2016-02-16 11:56:22:481962: root@contrail:/opt/contrail/utils#
```

AFBEELDING 61; CONTRAIL ERROR

Conclusie

De student heeft geprobeerd om de gehele omgeving opnieuw te installeren met de hoop de installatie van het pakket Contrail werkend te krijgen. Helaas is dit niet gelukt. De student kan concluderen dat het pakket nog niet volledig werkend is met een vCenter 5.5 omgeving. Ook ziet de student dat er in de scripts kleine foutjes zitten waardoor het duidelijk wordt dat het pakket nog niet helemaal klaar voor productie is in combinatie met een vCenter omgeving.

Conclusie

In dit hoofdstuk zullen de testresultaten van de verschillende pakketten naast elkaar worden gezet om zo een overzicht te krijgen van de behaalde resultaten. Hoe minder CPU performance er gebruikt wordt bij de routering, hoe beter het pakket reageert op de test. Voor de behaalde testresultaten van de pakketten wordt men doorverwezen naar tabel 28;

TABEL 28; PAKKET RESULTATEN

Getest pakket	CPU Performance bij routering van 1 GB/p.s	Doelstelling behaald? (Maximaal 70% CPU belasting bij een routering van 1 GB/p.s
VMware NSX	Maximaal 28,3 %	Ja
pfSense	Maximaal 53 %	Ja
Contrail	n.v.t	n.v.t

Zoals er in tabel 28 te zien is heeft het pakket VMware NSX de beste performance behaald tijdens het Proof of Concept.

Bijlage 8: Zelfreflectie

In deze zelfreflectie zal ik, Ricky Badal, terugkijken hoe mijn afstudeerperiode bij het bedrijf Sentia gegaan is.

In het begin was ik druk met het maken van mijn Plan van Aanpak. Dit heeft mij in mijn ogen veel tijd gekost omdat het mij niet altijd duidelijk was wat de opdracht precies was. Omdat ik wat later begonnen ben met mijn stage is gedurende het schrijven van het Plan van Aanpak de opdracht een klein beetje gewijzigd. Door deze wijziging raakte ik een beetje gestrest omdat ik dacht dat ik mijn Plan van Aanpak verkeerd had beschreven, terwijl deze al wel was ingeleverd.

Na overleg met de bedrijfsbegeleider is het duidelijk geworden dat de probleemstelling niet meer van toepassing is maar dat het om een kans gaat voor het bedrijf waarin er onderzocht wordt door de student wat de best mogelijke firewall is voor het bedrijf.

Nadat dit mij duidelijk werd kon ik mij volledig richten op het onderzoek en heb ik de verschillende firewalls kunnen vergelijken. Gelukkig ben ik tot de conclusie gekomen dat er eigenlijk niet zo heel veel gewijzigd is in mijn opdracht. De hoofd en deelvragen zijn hetzelfde gebleven. Alleen de kwestie moest opnieuw beschreven worden.

Tijdens het schrijven van de scriptie heb ik de samenhang van de deel documenten beschreven. De inhoud van de scriptie was er wel, alleen had ik mij nog niet gericht op de structuur van de scriptie. Omdat het mij niet helemaal duidelijk was wat voor structuur er in de scriptie moest komen heb ik een afspraak gemaakt met Jos van Dongen. Tijdens deze afspraak heeft Jos mij verteld wat er verwacht wordt van de scriptie en hoe ik de structuur hierop kan aanpassen. Na het aanpassen van de scriptie ben ik zelf gelukkig ook de structuur gaan begrijpen en is het mij duidelijk geworden wat de structuur, gekoppeld met de faseringen, van de scriptie hoort te zijn.

Terugkijkend naar mijn afstudeerperiode ben ik redelijk tevreden over mijn aanpak en de gemaakte afspraken. Als er één ding is wat ik anders zou aanpakken is dat ik eerder met mijn bedrijfsbegeleider wekelijkse afspraken zou willen maken. In het begin was het mij onduidelijk hoe ik de voortgang van het project kon duidelijk maken aan het bedrijf. Na een tijdje hierover nagedacht te hebben ben ik tot de conclusie gekomen om elke week een afspraak te maken met de bedrijfsbegeleider om hierin de voortgang en eventuele vragen te bespreken. Had ik dit eerder gedaan, dan had ik niet zoveel stress gehad tijdens de wijziging van de probleemstelling.

Uiteindelijk ben ik tevreden over het resultaat wat er opgeleverd is en ben ik trots op de documentatie die ik opgeleverd heb aan het bedrijf en de school. De afstudeerperiode is voor mij zeer leerzaam geweest omdat het de eerste keer is dat ik zelf een scriptie schrijf. Er zijn natuurlijk vele voorbeelden op het internet te vinden van een scriptie, echter is het mijn taak om de opdracht zo duidelijk mogelijk te verwerken in de scriptie en de faseringen, gekoppeld met de resultaten, op een zo duidelijk mogelijke manier te beschrijven.

De scriptie was voor mij een leuke uitdaging en ik twijfelde aan mezelf of ik de beloofde afspraken wel kon nakomen. Ik vind uitdagingen altijd leuk, vooral als deze leiden tot een goed resultaat, wat ik in mijn ogen wel bereikt heb en in het begin niet van mezelf had verwacht.