Scriptie Standaardisatie bij Constant IT

Constant IT

16 december 2014, Chris de Keijzer

Auteur: Chris de Keijzer
Opleiding: System & Network engineering
Studentnummer: 1591134
Telefoonnummer: 06-10181296
Datum: 16-11-2014
Versie: 1.0
Eerste examinator: Rienk van der Ploeg

DOCUMENTINFORMATIE

Documentbeheer en Goedkeuring

Versie	Auteur	Opmerkingen	Document Eigenaar	Datum
0.1	Chris de Keijzer	Eerste draft	Chris de Keijzer	3-11-2014
0.2	Chris de Keijzer	Feedback Suzanne verwerkt.	Chris de Keijzer	5-11-2014
0.3	Chris de Keijzer	Antwoorden deelvragen ingevuld tot aan PoC	Chris de Keijzer	16-11-2014
0.4	Chris de Keijzer	Feedback Suzanne verwerkt.	Chris de Keijzer	20-11-2014
0.5	Chris de Keijzer	Laatste inhoud toegevoegd. Snelle controle opmaak.	Chris de Keijzer	1-12-2014
0.6	Chris de Keijzer	Feedback Chris Leicher, Allard Borgart & Bas de Zeeuw verwerkt.	Chris de Keijzer	5-12-2014
1.0	Chris de Keijzer	Spellingscontrole en puntjes op de i.	Chris de Keijzer	15-12-2014

Dit document is beoordeeld door

Versie	Naam	Functie	Datum beoordeling
0.1	Suzanne van Wiltenburg	HRM manager	3-11-2014
0.3	Suzanne van Wiltenburg	HRM manager	20-11-2014
0.4	Chris Leicher	1ste versie gestuurd	20-11-2014
0.5	Chris Leicher	Docentbegeleider	4-12-2014
0.5	Bas de Zeeuw	Technisch begeleider	4-12-2014
0.5	Allard Borgart	Bedrijfsbegeleider	4-12-2014
0.6	Bas de Zeeuw	Technisch begeleider	11-12-2014
0.6	Chris Leicher	Docentbegeleider	

Dit document is goedgekeurd door

Versie	Naam	Functie	Datum beoordeling
1.0	Allard Borgart	Bedrijfsbegeleider	12-12-2014
1.0	Bas de Zeeuw	Technisch begeleider	12-12-2014

VOORWOORD

Voor u ligt mijn scriptie welke de afsluiting vormt van mijn bachelor System and Network engineering aan de Hogeschool Utrecht
Het onderzoek heeft plaatsgevonden vanaf 18 augustus tot 16 december 2014 en is uitgevoerd bij Constant IT gevestigd te Amsterdam. Het onderzoek richt zich op het creëren van een productvergelijking ten behoeve van besluitvorming en standaardisatie met betrekking tot netwerkapparatuur bij de klanten.

In dit voorwoord wil ik graag de docenten van de Hogeschool Utrecht bedanken voor de theoretische inzichten, kennis en inzet waarmee zij mij de laatste jaren hebben ondersteund.
Verder wil ik de volgende mensen bedanken voor hun inzet, begeleiding en betrokkenheid gedurende mijn afstudeerstage Allard Borgart, ICT manager, Bas de Zeeuw, technisch specialist en Suzanne van Wiltenburg, personeelsmanager.
Daarnaast wil ik graag Chris Leicher, de afstudeerbegeleider die mij is toegewezen door de Hogeschool Utrecht bedanken voor zijn begeleiding, inzet, feedback en geduld tijdens de stageperiode. Tot slot wil ik graag mijn familie en de collega's van Constant IT bedanken voor hun ondersteuning.

Chris de Keijzer

Weesp, december 2014

MANAGEMENTSAMENVATTING

Constant IT is snel gegroeid in de laatste jaren, echter blijkt nu dat door gebrek aan richtlijnen met betrekking tot levering van netwerkapparatuur er een wildgroei is ontstaan van allerlei merken. De wildgroei zorgt ervoor dat het moeilijk is om overzicht te houden van welk apparaat waar staat. Daarnaast kost het maken van technische documentatie veel tijd door de vele verschillende oplossingen. Ook nieuwe werknemers krijgen hiermee te maken, het duurt lang voordat nieuwe collega's alle verschillende configuraties kennen. Ook is het lastig om passend advies te geven aan klanten die netwerkapparatuur willen aankopen op basis van prijs-kwaliteitverhouding en hun requirements.

Om deze problemen op te lossen, wil Constant IT een aantal apparaten standaardiseren. Om dit te bereiken is er een productvergelijking nodig welke uiteindelijk leidt tot een selectie van meest geschikte apparaten. De productvergelijking en alle bijhorende aspecten zullen leiden tot een aantal verbeteringen in de organisatie zoals efficiënter werken en meer kennis binnen het bedrijf over een kleine selectie apparaten. Daarnaast zal het minder tijd kosten om alle technische documentatie te maken.

De probleemstelling van dit onderzoek luidt:
Op welke manier kan Constant IT apparatuur bestaande uit switches, routers en firewalls die geadviseerd wordt aan klanten per klantgroep standaardiseren, om de kwaliteit van de dienstverlening op een hoger niveau te krijgen, waarbij van één klantgroep de te standaardiseren apparatuur getest dient te worden?

Om antwoord te kunnen geven op deze hoofdvraag, zijn een aantal deelvragen opgesteld:

1. Wat zijn de ervaringen met apparatuur die nu geleverd wordt?
2. Hoe zou het management van Constant IT de bestaande klanten willen indelen in categorieën.
3. Welke technische en commerciële eisen en wensen worden er gesteld aan apparatuur door Constant IT en haar klanten, en welke waarde hebben deze?
4. Welke eisen wil het management van Constant IT in een beoordelingsmatrix meenemen?
5. Welke apparaten zijn het meest passend in de verschillende klantcategorieën?
6. Wat zijn de prijs/kwaliteit verhoudingen van apparaten die aan de technische en commerciële wensen voldoen?
7. Hoe kunnen de resultaten van het theoretisch onderzoek worden getoetst in de praktijk?

De klanten zijn ingedeeld in drie categorieën:

- Klein zakelijk (P1)
- MKB (P2)
- MKB+ (P3)

Alle klanten die een Service License Agreement (SLA) hebben met Constant IT zijn geplaatst in een model dat hun positie aangeeft binnen deze drie categorieën. Dit gaf antwoord op deelvraag 2. Vervolgens zijn er requirements vereisten opgesteld in samenwerking met de technische specialisten op netwerkgebied. Met behulp van interviews is achterhaald met welke apparaten men intern goede ervaring heeft. Dit zijn de volgende apparaten:

Routers	Firewalls	Switches L2	Switches L3
Draytek 2130	Watchguard XTM 26	Netgear GS108	Cisco Catalyst 2960
Draytek 2925Vn+	Watchguard XTM 26	Cisco SG200	
	Watchguard XTM33	Cisco SG300	

Tabel 1 Producten met goede ervaringen

Voor iedere categorie is een aparte set eisen opgesteld. Alle eisen hebben een niveau toegewezen gekregen met behulp van de MoSCoW methode.

Het vergelijkende onderzoek heeft vervolgens de requirements die Constant IT stelt aan de hand van long- en shortlists vergeleken met een groep apparaten. Uiteindelijk is er in overleg met het management van Constant IT besloten om de losse beoordelingsmatrix achterwege te laten en deze te integreren met de shortlist.
De apparaten op de shortlist zijn met behulp van onderstaande puntenverdeling met elkaar vergeleken.

Type eis	Waarde
Must have	10 punten
Should have	5 punten
Could have	2 punten
Goede ervaringen Constant IT	20 punten

Tabel 2 Puntenverdeling vergelijking

Daarna is er voor de apparaten op basis van bovenstaande puntenverdeling een prijs-kwaliteitverhouding vastgesteld. Hoewel de prijs-kwaliteitverhouding niet leidend is, is deze wel in acht genomen bij de keuze voor apparaten. De volgende apparaten kwamen als meest geschikt uit de vergelijking:

Categorie	Switches	Prijs-kwaliteitverhouding	Routers/firewalls	Prijs-kwaliteitverhouding
P1	Linksys LGS124	2,04	Draytek Vigor 2130	2,12
P2	Cisco Sg300-28	2,12	Watchguard XTM26	1,77
P3	SG500/SG500x	3,45/5,41	Watchguard XTM33/330-	5,74/7,33

Tabel 3 Resultaten onderzoek
***Prijs-kwaliteitverhouding, lager is beter**

Om de kwaliteit van het onderzoek te waarborgen is er een proof of concept gedaan om de theoretisch meest geschikte apparaten in de praktijk te testen. Het proof of concept met de Watchguard XTM26 en Cisco SG300 heeft aangetoond dat deze apparaten goed ingezet kunnen worden bij klanten. Daarnaast is er nog een losstaande casus uitgevoerd, binnen de proof of concept, met de Watchguard XTM26. Hierbij is getest hoe dit apparaat kan helpen in de verdediging tegen malware. Deze casus heeft uitgewezen dat de verschillende optionele beveiligingsdiensten, die tegen een meerprijs af te nemen zijn, gezamenlijk een zeer effectieve verdediging vormen tegen malware-aanvallen. Als laatste is er een flowchart ontwikkeld om de afdeling Sales te ondersteunen in de besluitvorming, er kan met behulp van enkele antwoorden besloten worden welk apparaat geleverd dient te worden aan klanten. De hoofdvraag is uiteindelijk beantwoord door een aantal building blocks te maken. Deze building blocks bevatten per klantcategorie het meest geschikte apparaat en een basisconfiguratie.
Op basis van de resultaten van het onderzoek zijn de volgende aanbevelingen gedaan aan Constant IT:

1. Test de overige apparaten die als meest passend uit het theorie onderzoek komen in een proof of concept.
2. Gebruik de opgestelde building blocks, lever de aanbevolen apparaten en bouw basis configuraties op zoals beschreven;
3. Biedt bij Watchguard firewalls altijd optioneel een volledige security bundel aan, hierbij is het belangrijk dat men uitlegt wat de bundel kan bieden;
4. Houdt het onderzoek bij, apparaten die nu het best passen kunnen in de toekomst vervangen worden door anderen. Daarnaast zouden er nieuwe building blocks kunnen ontstaan.

De aanbevelingen leiden uiteindelijk tot minder diversiteit van netwerkapparatuur bij de klanten van Constant IT, waardoor het beheer voor Constant IT vereenvoudigd wordt. Daarnaast zullen de werknemers meer kennis verkrijgen van de apparaten en kunnen problemen sneller opgelost worden. De building blocks en het onderzoek dat tot de bouw van de building blocks leidde, zijn zo opgesteld dat deze eenvoudig gewijzigd of uitgebreid kunnen worden met nieuwe categorieën

INHOUDSOPGAVE

1 Inleiding 10
2 De organisatie 11
2.1 Bedrijfsprofiel 11
2.2 De positie binnen Constant IT 12
3 De opdracht 13
3.1 Aanleiding 13
3.2 Doelstelling 13
3.3 Hoofdvraag en deelvragen 14
3.4 Producten 14
3.5 Projectfasering 15
3.6 De aanpak 16
3.6.1 Fase 1 - Voorbereiding 16
3.6.2 Fase 2 - Inventariseren 16
3.6.3 Fase 3 - vergelijkend Onderzoek 16
3.6.4 Fase 4 - Ontwerp & advies 17
3.6.5 Fase 5 - Proof of concept en afronding 17
3.7 Gebruikte methoden en technieken 17
4 Verdeling van de klanten 18
5 De eisen 20
5.1 Globale eisen 20
5.2 Specifieke eisen 21
5.2.1 Switches 22
5.2.2 Routers 24
6 De ervaringen van Constant it met de huidige producten 26
6.1 Routers 26
6.2 Firewalls 26
6.3 Switches 26
7 De uiteenzetting van de vergelijking 27
8 Prijs-kwaliteitsverhoudingen en shortlists 28
8.1 Shortlist switch p1 28
8.2 Shortlist router p1 29
8.3 Shortlist switch p2 30
8.4 Shortlist router & firewalls p2 31
8.5 Shortlist switch p3 32
8.6 Shortlist router & firewalls p3 33
9 De aanbevolen apparaten 34
9.1 Switch P1 34
9.2 Router P1 34

9.3 Switch P2 35
9.4 Router P2 35
9.5 Switch P3 35
9.6 Router P3 36
9.7 Flowchart 37
10 Proof of concept 38
10.1 De testopstelling 38
10.2 Resultaten van de tests 39
10.3 Resultaten Casus malware blokkeren 39
11 Building Blocks 40
12 Conclusie 41
13 Aanbevelingen 41
Bijlage 1: Plan van aanpak .....
Bijlage 2: Evaluatie chris de keijzer .....
Bijlage 3: Requirements .....
Bijlage 4: Vergelijkend onderzoek .....
Bijlage 5: Testplan .....
Bijlage 6: Building blocks .....

VERKLARENDE WOORDENLIJST

ACL	Access Control Lists zijn lijsten die door routers en firewalls gebruikt worden om via regels toegang geven of ontzeggen tot bepaalde netwerkbronnen.
All-in-one oplossing	Eén oplossing die voorziet in alle behoefte, binnen het project wordt hiermee een firewall bedoeld die ook dienst kan doen als router.
APT Blocker	De Advanced Persistent Threat blocker is een Watchguard subscription service welke malware die nog niet herkend worden door virusscanners kan herkennen als schadelijk programma. (Watchguard, 2014)
CLI	Command Line Interface waarmee via tekstinvoer commando's aan apparatuur wordt doorgevoerd.
Multi WAN	Multi WAN apparatuur heeft twee ingangen voor WAN verbindingen en kan deze simultaan gebruiken.
Gateway Antivirus	De antivirus oplossing die op de Watchguard firewalls draait, dit is een Watchguard subscription service
High availability	Een oplossing die altijd beschikbaar is doordat er failover en clustering gebruikt wordt.
IPS	Intrusion Prevention systems scannen verkeer op de meest gebruikte protocollen en beschermt tegen spyware, SQL injecties en buffer overflows. Nieuwe aanvallen kunnen snel herkend worden omdat er periodiek updates van Watchguard worden gedownload met de nieuwste "signatures".
Java	Software van een derde partij die in sommige gevallen noodzakelijk is om bepaalde scripts op webpagina's te draaien.
LAN	Local Area Network, dit is het eigen interne netwerk
Layer2	Hiermee wordt layer 2 van het OSI model bedoeld. Veel switches werken op deze laag en kennen dus geen IP adressen maar alleen "frames" en switching gebeurd op basis van MAC adres. (Alani, 2014)
Layer3	Layer 3 is de laag waarop routers en logische paden ofwel routing tables hun werk doen. Deze voorzien in routes op IP basis naar andere netwerkapparatuur. (Alani, 2014)
Longlist	Een lijst met apparaten die voldoen aan de globale requirements.
Managed switch	Een switch die zoals de naam zegt te beheren is, hierop kunnen diepgaande configuraties gemakt worden.
Out of the box	Iets dat werkt zonder dat daar iets voor gedaan hoeft te worden.
Proof of Concept	Een testopstelling die bewijs levert van de werking van een concept.
QoS	Quality of Service gaat om het garanderen van bepaalde services op het netwerk door prioriteiten te stellen. Denk bijvoorbeeld aan VoIP verkeer dat stabiel moet blijven.
Reputation enabled defense	Blokkeren van websites door middel van informatie die verkregen wordt via de cloud, dit is een Watchguard subscription service.
Requirements	De eisen, voor dit project zijn deze eerder gedefinieerd in het requirements document.
Shortlist	Een lijst met apparaten die aan eisen en wensen voldoen en waar eventueel goede ervaringen mee zijn. Deze voorkeurslijst is gebaseerd op de longlist
Sizing	Deze term houdt in dat apparatuur passend moet zijn bij een klantcategorie. Denk aan voldoende poorten/doorvoersnelheid.
Smart switch	Een smart switch vult het gat tussen unmanaged en managed switches. Het is een semi-managed switch welke eigenschappen heeft van allebei.
Stacking	Het stapelen van apparatuur, door stacking kunnen twee apparaten (of meer) samenwerken als één.

Subscription based licensing	Dit is het verkrijgen van licenties waarvoor jaarlijks of maandelijks betaald dient te worden. Dit komt vaak voor bij apparatuur die vaak geüpdatet dient te worden.
TMAP	TMAP is een methode om gestructureerd te testen in een goed te begrijpen en beheerbaar proces. (Sogeti Nederland B.V, 2012)
Unmanaged switch	Een switch die uit de box werkt, er valt niets in te stellen en functioneert nadat de stekker is ingeplugd.
VoIP	Het Voice over Internet Protocol is bellen via het netwerk.
VPN	Een Virtual Private Network is een verbinding die via het internet (WAN) naar een andere locatie loopt waarmee het lijkt alsof er in het LAN gewerkt wordt. Deze verbindingen zijn veelal versleuteld.
VRRP	Dit protocol ondersteund in redundantie, VRRP staat dan ook voor Virtual Router Redundancy Protocol. VRRP wijst een master router aan een één of meerdere backup routers. Op deze manier is een verbinding altijd beschikbaar. Dit protocol werkt ook op (high end) switches.
WAN	Met een Wide Area Network wordt het netwerk bedoeld vanaf het eigen modem. De netwerken van de internetproviders zijn dus “ wan)
WebBlocker	Met behulp van deze Watchguard subscription service kunnen specifieke websites of volledige categorieën (zoals social media) geblokkeerd worden.

1 INLEIDING

Dit onderzoek is uitgevoerd in opdracht van Constant IT en is het resultaat van de afstudeeropdracht van Chris de Keijzer aan de Hogeschool Utrecht. Deze scriptie bevat de context waarbinnen de afstudeeropdracht is uitgevoerd alsmede de resultaten van de verschillende onderzoeksvragen.
Constant IT is in de laatste jaren sterk gegroeid echter zijn er bij opleveringen van netwerkapparatuur zelden dezelfde apparaten gebruikt. Hierdoor wordt het beheer van al deze configuraties steeds complexer.
Het doel van het onderzoek is het terugdringen van diversiteit van netwerkconfiguraties bij klanten van Constant IT. Om dit te bereiken wordt er een productvergelijking gedaan die een aantal meest geschikte apparaten op levert voor verschillende klant categorieën.

In hoofdstuk twee zal er gestart worden met algemene informatie over Constant IT. Hoofdstuk drie bevat de opdracht, doelstellingen, onderzoeksvragen en fasering zoals gespecificeerd in het plan van aanpak. Hoofdstuk vier behandeld de onderverdeling van de klanten waarop de productvergelijking is gebaseerd en hoofdstuk vijf beschrijft de eisen die gesteld zijn aan de apparatuur. Hoofdstuk zes behandeld de ervaringen van Constant IT met apparatuur die nu geleverd wordt. Het onderzoek is uiteengezet in de hoofdstukken zeven, acht en negen. In hoofdstuk zeven wordt de puntentoekenning besproken, gevolgd door de shortlists en prijs-kwaliteitverhoudingen in hoofdstuk acht. Hoofdstuk negen bevat de eindresultaten van het theoretisch onderzoek.
Het proof of concept en de resultaten daarvan worden beschreven in hoofdstuk tien gevolgd door de building blocks in hoofdstuk elf.
In hoofdstuk 12 wordt de scriptie afgerond met een conclusie en aanbevelingen.
Naast al deze hoofdstukken zijn er ook nog een aantal bijlagen aanwezig welke diverse malen aangehaald worden.
Bijlage één bevat het plan van aanpak van het onderzoek en bijlage twee bevat een persoonlijke evaluatie van het verloop van het onderzoek. De verschillende beroepsproducten, zoals de requirements, het vergelijkend onderzoek en het testplan met de testresultaten zijn te vinden in de bijlagen drie, vier en vijf. Bijlage zes bevat de building blocks.

2 DE ORGANISATIE

Dit hoofdstuk bevat algemeen informatie over Constant IT en de werkzaamheden die uitgevoerd worden.

2.1 BEDRIJFSPROFIEL

Constant IT is in 1996 opgestart door Robin Kuipers. Robin ging tijdens zijn studententijd, onder de naam “Man en Muis”, naar particuliere klanten om computerproblemen op te lossen. Na een aantal jaar groeide het bedrijf uit tot een dienstverlenend bedrijf, dat naast particulieren ook het midden- en kleinbedrijf (MKB)van Amsterdam voorzag van betrouwbare service. Uiteindelijk is er gekozen voor een naamswijziging die meer professionaliteit uitstraalde, waarmee Constant IT was geboren.

Constant IT voorziet nog steeds het (MKB) van systeembeheer services en heeft een team dat bestaat uit achttien medewerkers in diverse lagen van de organisatie. Op dit moment beheerd Constant IT de infrastructuur van ongeveer 200 klanten die variëren van kleine eenmanszaken tot bedrijven met ongeveer 200 medewerkers. Alle werkzaamheden worden gedaan in de omgeving van Amsterdam, waardoor er een diverse klantenkring is ontstaan met klanten in (onder andere) de financiële sector, de horeca en de non-profitsector.

Het geleverde dienstenpakket bestaat op dit moment uit:

- Systeembeheer (particulier en zakelijk);
- Consultancy en Auditing;
- Cloud diensten zoals hosted exchange, desktop online, online back-up en VoIP[1];
- Webhosting.

Constant IT groeit voortdurend en beoogt tegelijkertijd om efficiënter te werken en de organisatie volwassener te maken. Deze ambities zijn samengevoegd onder de naam 'Constant IT 2.0'.
Het bedrijf heeft een aantal doelstellingen voor de toekomst:

- Constant IT wil één van de meest toonaangevende ICT-dienstverleners van Amsterdam en omstreken worden;
- Constant IT wil, zowel intern als extern, een zeer professionele organisatie neerzetten;
- Constant IT wil een aantrekkelijke werkgever zijn voor getalenteerde ICT’ers;
- Constant IT wil alle soorten klanten kunnen bedienen, met zowel standaard- als maatwerkoplossingen;
- Constant IT wil flexibel zijn om snel in te kunnen springen op technologische ontwikkelingen;
- Constant IT wil efficiënter werken.

[1] http://www.constant.it/diensten

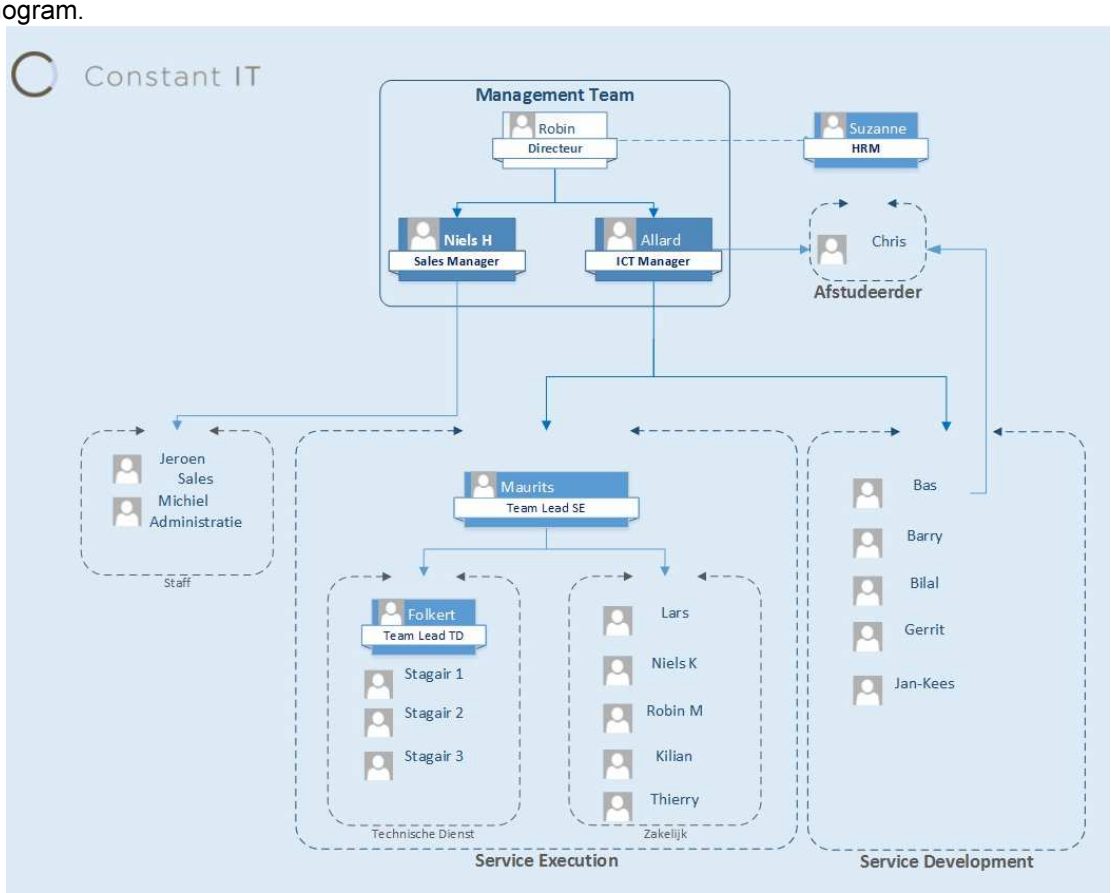
2.2 DE POSITIE BINNEN CONSTANT IT

Tijdens de afstudeerperiode is er meegedraaid op de afdeling systeembeheer. Deze afdeling valt onder te verdelen in twee subafdelingen namelijk:

Service Development
Op deze afdeling wordt gewerkt aan de grotere projecten, worden nieuwe services ontwikkeld en worden geëscaleerde incidenten opgelost. Voorbeelden van de projecten zijn het migreren van servers, of het vernieuwen en/of uitbreiden van de netwerkinfrastructuur. Daarnaast functioneert Service Development ook als vraagbaak voor de afdeling Service Execution. Service development (SD) functioneert als tweedelijns support waar complexe problemen die niet door de Service Execution afdeling opgelost kunnen worden.

Service Execution.
Deze afdeling houdt zich bezig met reactief beheer. Klanten die problemen ervaren met de dienstverlening van Constant IT kunnen bellen of e-mailen naar het bedrijf, waarna er een ticket aangemaakt wordt in het ticketsysteem. Afhankelijk van het service level agreement (SLA) dat is afgesproken met de klant in kwestie, wordt de prioriteit bepaald van het ticket. Omdat Service Execution (SE) het eerste aanspreekpunt is, wordt deze afdeling gezien als eerstelijns support voor problemen die klanten ervaren. Iedereen heeft binnen Constant IT de titel *Technical Specialist* om gelijkheid te creëren. In figuur 1 is het organogram van Constant IT opgenomen.

De afstudeerder
Aansturing van de afstudeerder is gedaan door zowel Bas de Zeeuw van de Service Development afdeling als ICT manager Allard Borgart. Zie ook de positie van de afstudeerder in onderstaande organogram.



Figuur 1 Organogram Constant IT

3 DE OPDRACHT

In hoofdstuk 3 wordt de opdracht zoals tot stand gekomen in het plan van aanpak beschreven, er wordt teruggekeken op de aanleiding en de doelstellingen.

3.1 AANLEIDING

Constant IT is de afgelopen jaren snel gegroeid: er zijn meer klanten, meer werknemers en meer diensten. Bij veel van haar klanten heeft Constant IT de infrastructuur opgebouwd of aangepast, maar zelden worden hier dezelfde apparaten voor gebruikt. Nu blijkt dat het beheer van de geleverde apparatuur bij verschillende klanten steeds complexer wordt. Dit komt door het gebrek aan een standaard op het gebied van netwerkapparatuur. Door beperkte kennis over het volledige assortiment aan apparaten, ontstaan de volgende problemen op de technische en sales afdelingen.

- Bij elk apparaat kan in potentie een ander probleem ontstaan, waardoor er incidenten kunnen ontstaan;
- Het is onmogelijk om voor elk apparaat technische documentatie bij te houden;
- Het is onduidelijk welk apparaat bij een klant staat;
- Inwerken van nieuwe collega's vergt meer tijd door de verschillende configuraties bij de verschillende klanten;
- Besluitvorming vanuit de sales afdeling verloopt traag;
- Het is lastig om passend advies geven op basis van de prijs-kwaliteitverhouding en requirements de vereisten van de klant.

Zoals eerder genoemd, wil Constant IT graag efficiënter gaan werken en willen zij apparaten gaan standaardiseren om de wildgroei van apparaten tegen te gaan. In de visie van Constant IT blijft er met behulp van standaardisatie een kleine selectie geteste apparaten over, die geleverd zullen worden aan klanten. Door deze standaardoplossingen aan te bieden en deze aan te passen aan de budgeten van de klanten, zal de keuze voor een apparaat sneller gemaakt worden.

3.2 DOELSTELLING

Dit onderzoek heeft als doel om de kwaliteit van de dienstverlening te verhogen, het beheer te vereenvoudigen en een kostenverlaging tot stand te brengen. Dit alles zal gedaan moeten worden door het aanbieden van standaard dienstverlening. De kwaliteit van dienstverlening bestaat volgens Constant IT uit:

- Het aantal incidenten;
- De doorlooptijd van incidenten;
- De doorlooptijd van verkooptrajecten;
- De stabiliteit en performance van de apparatuur bij klanten;
- Oplossingen aanbieden die aansluiten bij de huidige en toekomstige vereisten van de klant.

De verwachting is dat dit onderzoek uiteindelijk zal leiden tot een efficiënter niveau van werken. Dit heeft een aantal bijkomende voordelen, zoals:

- Sneller en efficiënter werken op de afdelingen die geraakt worden door dit afstudeerproject;
- Werknemers hebben diepgaande kennis van een kleine selectie apparaten, waardoor de doorlooptijd van incidenten verkort en de klanttevredenheid groeit;
- Het opzetten van een kennisbank voor een klein aantal apparaten kost minder tijd;
- Het wordt eenvoudiger om interne kennisoverdracht te laten plaatsvinden.

Het onderzoek zal uitgevoerd worden in de vorm van productvergelijkingen en praktijktests van apparaten. Deze apparaten zullen vervolgens gestandaardiseerd worden in de vorm van een building block (TOGAF) (Open Group (Building Blocks), 2011).

Uiteindelijk zal deze standaardisatie leiden tot een consistent en voorspelbaar proces met betrouwbare resultaten op de gebieden van beheer en verkoop.
Om het onderzoek succesvol te kunnen noemen, moet er minimaal een productvergelijking gecreëerd zijn die voorziet in richtlijnen over juist advies aan klanten en een proof of concept van de apparaten die als meest geschikt uit de vergelijking komen.

3.3 HOOFDVRAAG EN DEELVRAGEN

De volgende hoofdvraag en deelvragen zijn opgesteld om de doelstelling van het onderzoek te kunnen verwezenlijken.

Hoofdvraag
Op welke manier kan Constant IT apparatuur bestaande uit switches, routers en firewalls die geadviseerd wordt aan klanten per klantgroep standaardiseren, om de kwaliteit van de dienstverlening op een hoger niveau te krijgen, waarbij van één klantgroep de te standaardiseren apparatuur getest dient te worden?

Deelvragen

1. Wat zijn de ervaringen met apparatuur die nu geleverd wordt?
2. Hoe zou het management van Constant IT de bestaande klanten willen indelen in categorieën.
3. Welke technische en commerciële eisen en wensen worden er gesteld aan apparatuur door Constant IT en haar klanten, en welke waarde hebben deze?
4. Welke eisen wil het management van Constant IT in een beoordelingsmatrix meenemen?
5. Welke apparaten zijn het meest passend in de verschillende klantcategorieën?
6. Wat zijn de prijs/kwaliteit verhoudingen van apparaten die aan de technische en commerciële wensen voldoen?
7. Hoe kunnen de resultaten van het theoretisch onderzoek worden getoetst in de praktijk?

3.4 PRODUCTEN

Tijdens de afstudeeropdracht zijn de volgende producten opgeleverd:

Producten voor de Hogeschool Utrecht:

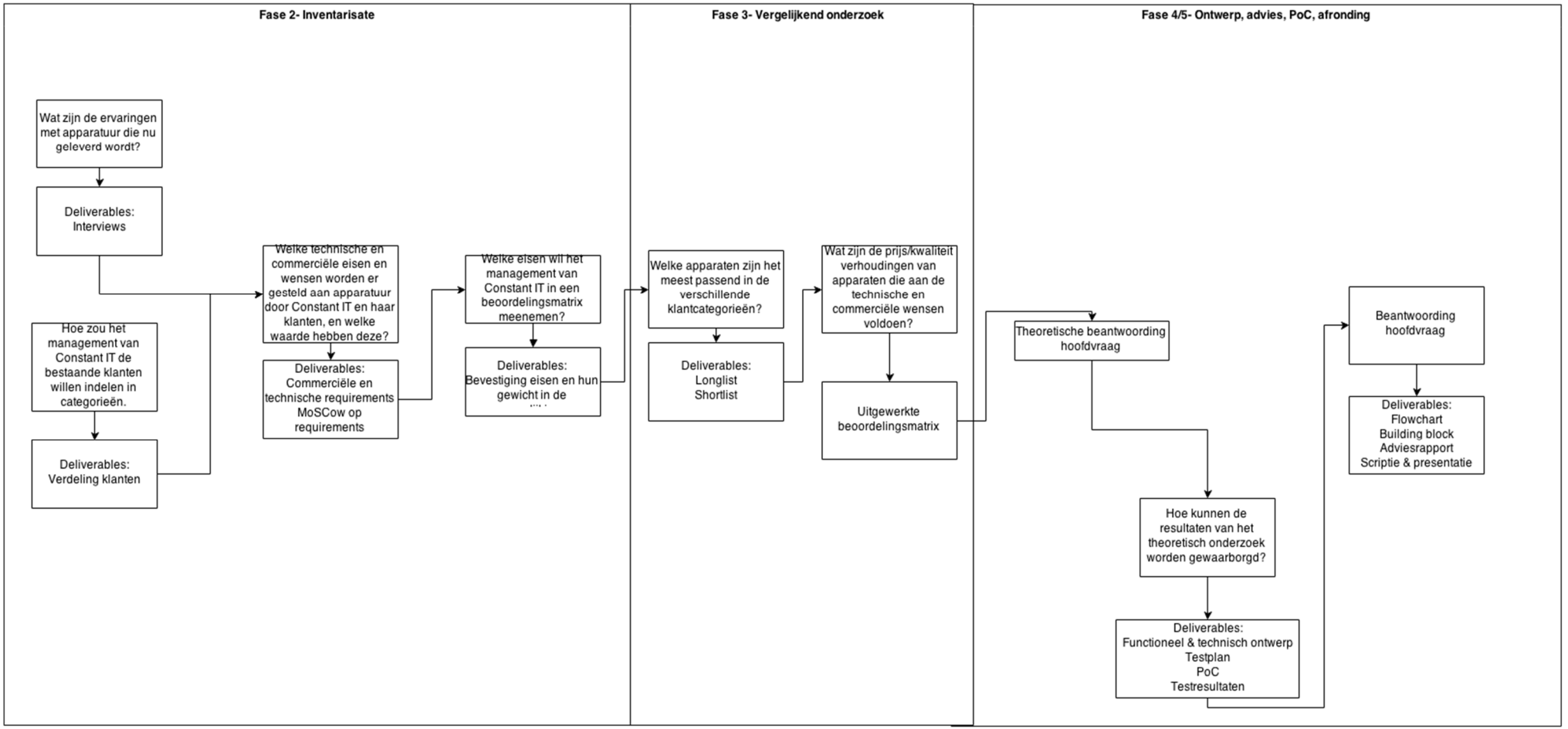
- Plan van Aanpak;
- Scriptie;
- Presentatie van de scriptie.

Producten voor Constant IT:

- Plan van aanpak;
- Requirements analyse;
- Productvergelijking;
- Functioneel ontwerp;
- Technisch ontwerp;
- Testplan;
- Proof of concept;
- Flowchart;
- Adviesrapport (scriptie).

3.5 PROJECTFASERING

Het project is verlopen volgens de waterval methode, dit betekend dat de onderdelen opvolgend worden uitgevoerd. (Royce, 2003) In de figuur hieronder wordt de waterval van dit project weergegeven.



Figuur 2 Fasering van het project

3.6 DE AANPAK

Het project is verdeeld in een aantal fasen: de voorbereiding, de inventarisatie, het vergelijkend onderzoek, het ontwerp, het advies en ten slotte het proof of concept en afronding van het onderzoek.

3.6.1 FASE 1 - VOORBEREIDING

In deze fase is het plan van aanpak van het project gemaakt. Het plan van aanpak (PvA) is gebaseerd op de template die is aangeleverd door de Hogeschool Utrecht.

3.6.2 FASE 2 - INVENTARISEREN

In de inventarisatiefase zijn de klanten gecategoriseerd. Tevens zijn de eisen en wensen (requirements) van Constant IT, via brainstormsessies, achterhaald. De eisen en wensen zijn met behulp van de MoSCoW-methode geprioriteerd. Daarnaast zijn de ervaringen die Constant IT heeft met de huidig geleverde apparatuur in kaart gebracht via interviews met open vragen. Deze fase heeft geleid tot een document met requirements welke te vinden is in bijlage drie.

In deze fase worden de volgende deelvragen beantwoord:

- Wat zijn de ervaringen met de apparatuur die nu geleverd worden?
- Hoe zou het management van Constant IT de bestaande klanten willen indelen in categorieën?
- Welke technische en commerciële eisen en wensen worden gesteld aan de apparatuur door Constant IT en haar klanten, en welke waarde hebben deze?

3.6.3 FASE 3 - VERGELIJKEND ONDERZOEK

De onderzoeksfase bestaat uit het vergelijken van apparaten. Dit wordt gedaan met behulp van de methode 'pakketselectie HU' (Utrecht, 2013). Dit betekent dat er longlists en shortlists zijn opgesteld op basis van de requirements uit fase twee. Er is deskresearch gedaan om de benodigde informatie over de vergeleken apparaten en hun features te verkrijgen. De resultaten van de longlists en shortlists leiden uiteindelijk tot een aantal meest geschikte apparaten en prijs-kwaliteitverhoudingen om dit te ondersteunen. Het vergelijkend onderzoek is te vinden in bijlage vier.

In deze fase worden de volgende deelvragen beantwoord:

- Welke eisen wil het management van Constant IT in een beoordelingsmatrix meenemen?
- Welke apparaten zijn het meest passend bij de verschillende klantcategorieën?
- Wat zijn de prijs-kwaliteitverhoudingen van apparaten die aan de technische en commerciële wensen voldoen?

3.6.4 FASE 4 - ONTWERP & ADVIES

In deze fase wordt er een theoretisch antwoord op de hoofdvraag gegeven en wordt er een opzet gemaakt voor het advies. Om de theoretische resultaten te ondersteunen met praktische resultaten, is er een proof of concept voorbereid. Hiervoor is een op TMAP gebaseerd testplan geschreven, en zijn er functionele en technische ontwerpen gemaakt. Daarnaast is er ook voor apparatuur gezorgd waarmee getest wordt, dit is apparatuur die als meest geschikt uit het vergelijkend onderzoek is gekomen. Het testplan is te vinden in bijlage vijf.

3.6.5 FASE 5 - PROOF OF CONCEPT EN AFRONDING

Het project wordt in deze fase afgerond. Er is een proof of concept uitgevoerd, waarmee de theoretische resultaten die zijn verkregen in de andere fasen gecontroleerd kunnen worden. De resultaten van de tests zijn beschreven in bijlage vijf. Naast de proof of concept wordt in deze fase de scriptie ook afgerond, de presentatie gemaakt en alle informatie aan de opdrachtgever overhandigd.

In deze fase wordt de volgende deelvraag beantwoord:

- Hoe kunnen de resultaten van het theoretisch onderzoek worden getoetst in de praktijk?

3.7 GEBRUIKTE METHODEN EN TECHNIEKEN

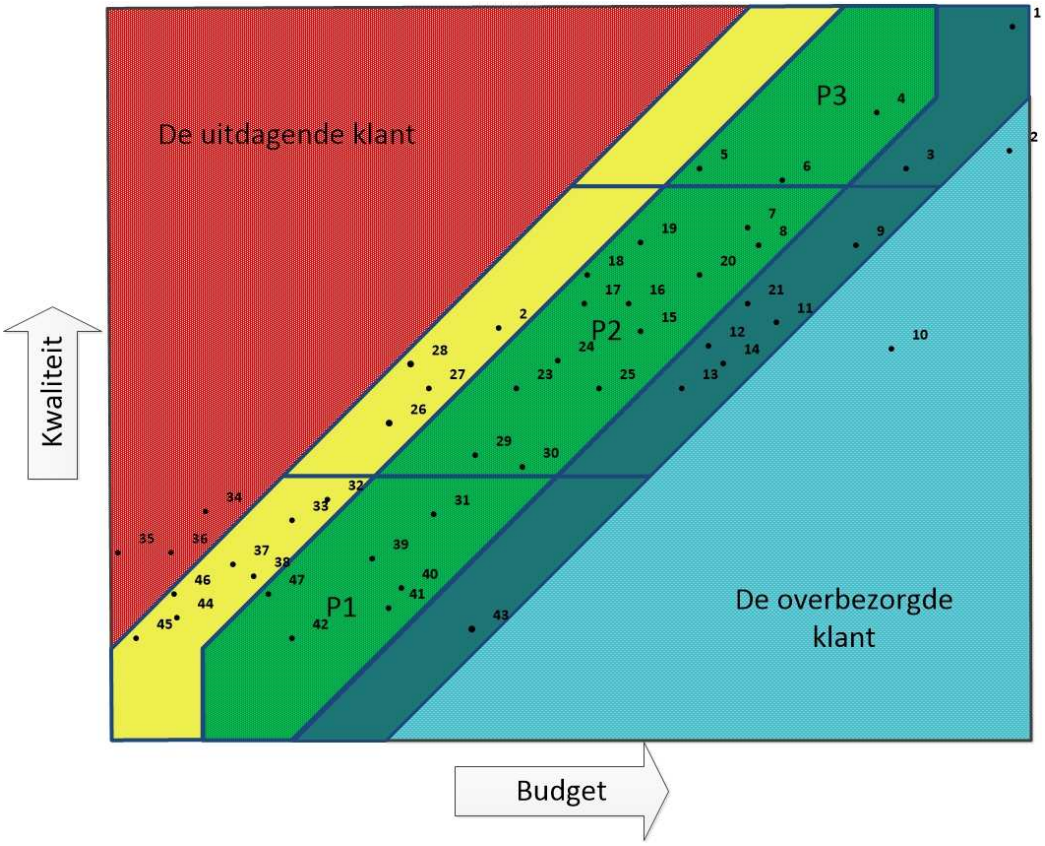
Dit hoofdstuk beschrijft kort welke methoden en technieken met welk doel zijn gebruikt

Methode of techniek	Doel
Deskresearch	Onderzoek naar apparaten, eisen of methoden.
Interviews	Er zijn open interviews gehouden om gebruikerservaringen te achterhalen.(Steehouder, 2012)
TOGAF(building blocks)	Building blocks zijn gebruikt voor de standaardisatie en bevatten een configuratie. (Open Group (Building Blocks), 2011)
Moscow + requirement prioritization	Gebuikt om prioriteiten aan te geven voor de requirements. (International Institute of Buisiness Analysis, 2009)
Productvergelijking(Pakketselectie HU) + beoordelingsmatrix	De longlists en shortlists zijn gebaseerd op de methode van Harry Beerlage(Utrecht, 2013)
Functioneel ontwerp en technisch ontwerp	Deze technieken zijn gebruikt om het proof of concept voor te bereiden
TMAP en testplan	Ter voorbereiding op het proof of concept is er een testplan geschreven op basis van de TMAP methode. (Sogeti, 2011)
Proof of concept	Er is een proof of concept uitgevoerd om de resultaten van het theoretisch onderzoek te waarborgen(Investorwords, sd)
Gantt chart	De Gantt chart is gebruikt om de planning te maken en bij te houden. (Bloomsbury Buisiness Library, 2007)
Flowchart	De flowchart is gebruikt om de onderzoeksresultaten over te dragen naar Constant IT
Training	Er is training geweest in de vorm van een scriptie bootcamp op de hogeschool Utrecht. Er is ook een driedaagse training geweest bij Watchguard om de apparaten te leren kennen ter voorbereiding op het proof of concept

Tabel 4 Methoden en technieken

4 VERDELING VAN DE KLANTEN

Bij Constant IT bestaat een grote diversiteit aan klanten. Om efficiënter te kunnen werken is besloten om al deze klanten in te delen in verschillende categorieën. Met deze categorieën kan dan vervolgens gewerkt worden om de productvergelijking te realiseren. In dit hoofdstuk wordt antwoord gegeven op de deelvraag: *Hoe zou het management van Constant IT de bestaande klanten willen indelen in categorieën*?
Constant IT heeft een groot aantal klanten die onderling sterk van elkaar verschillen. Met het oog op de productvergelijking, is in overleg met de opdrachtgever besloten om de klanten eerst te verdelen in categorieën. Aan deze categorieën worden vervolgens specifieke eisen gekoppeld. Er is aan de hand van brainstormsessies met de opdrachtgever een model ontwikkeld die de positie van klanten aangeeft. Het model is vervolgens, samen met het management van Constant IT, ingevuld. De verdeling van de klanten is gedaan op basis van het niveau van de kwaliteit dat een klant verwacht, en het budget dat zij beschikbaar hebben voor het aanleggen van een IT-infrastructuur. Omdat Constant IT niet wil dat namen van klanten gepubliceerd worden is dit model geanonimiseerd.



Figuur 3 Verdeling klanten Constant IT

In de productvergelijking wordt de 'realistische klant' gebruikt, deze klantgroep is in het model met groen aangegeven. Bij deze klantcategorie wordt ervan uitgegaan dat zij willen betalen voor wat zij nodig hebben. Er zijn uiteraard ook uitzonderingen op de realistische klant, deze worden aangegeven in de hoeken met de 'uitdagende' en 'overbezorgde' klantgroepen. Hoe verder een klant richting de 'uitdagende hoek' zit, hoe meer deze klant overtuigd moet worden om een investering te doen. Een 'overbezorgde klant' is het compleet tegenovergestelde van een 'uitdagende klant'. Deze klant denkt dat een duurder apparaat een beter apparaat betekent, terwijl de technische eisen dit niet verantwoorden. Hierdoor moet deze klant geadviseerd worden om hem te beschermen tegen te dure aankopen. Het model is ingevuld met behulp van het management van Constant IT en gelimiteerd tot klanten die een Service Level Agreement hebben met Constant IT.

De in de groene lijn aanwezige klantgroepen, de 'realistische klanten', zijn de klanten waar bij de productvergelijking op is geconcentreerd. Deze klanten zijn verdeeld in drie categorieën:
De in de groene lijn aanwezige klantgroepen, ofwel de realistische klanten zijn de klanten waar de productvergelijking zich op heeft geconcentreerd. Het resultaat van de verdeling zijn een aantal klantcategorieën waar eisen en wensen aan gekoppeld worden. Er worden drie verschillende categorieën onderkent:

P1: “Klein zakelijk”
Dit zijn de kleinste klanten, zowel budgettair als qua eisen. Deze klanten zoeken eenvoudige apparatuur voor een goede prijs. De apparatuur moet voorzien in basisconnectiviteit.

P2 “MKB”
Het midden- en kleinbedrijf vormt het grootste deel van de klanten van Constant IT. Deze klanten houden zich druk bezig met de continuïteit van de bedrijfsvoering, waardoor er vanuit het IT perspectief complexere eisen en wensen ontstaan.

P3 “MKB+”
Dit zijn de grootste klanten van Constant IT. Het apparatuur van deze klanten grenst net onder het 'Enterprise'-niveau. De eisen verschillen niet veel die van de P2 categorie maar omdat er meer werkplekken zijn die aangestuurd moeten worden, zal er apparatuur met snellere hardware moeten worden aangeschaft.

5 DE EISEN

In dit hoofdstuk worden de eisen en wensen (requirements) per klantcategorie behandeld die in het document met requirements zijn opgenomen. Daarnaast wordt er deels een antwoord gegeven op de deelvraag: *Welke technische en commerciële eisen en wensen worden er gesteld aan apparatuur door Constant IT en haar klanten, en welke waarde hebben deze?* Deze deelvraag is beantwoord door brainstorm sessies te houden met het management en de netwerkspecialisten van Constant IT.

5.1 GLOBALE EISEN

Om tot een longlist te kunnen komen, zijn er een aantal basiseisen gedefinieerd voor de te vergelijken apparaten die op de verschillende categorieën van toepassing zijn. Deze eisen staan samengevat in de onderstaande tabellen. De volledige lijst met eisen en de rationale achter deze eisen is terug te vinden in paragraaf 3.1 van bijlage drie.

P1					
Eisen			**Eisen**		
Routers/Firewalls	**Commercieel**	**Technisch**	**Switches L2/L3**	**Commercieel**	**Technisch**
Prijs tot 200	V		Prijs tot 150	V	
Binnen 7 dagen leverbaar	V		Binnen 7 dagen leverbaar	V	
Tot aan 15 gebruikers	V	V	Vanaf 16 poorten	V	V
Goede beoordeling externe partij		V	PoE versie beschikbaar		V
Vlan tagging		V			

Tabel 5 Globale eisen P1 categorie

P2					
Eisen			**Eisen**		
Routers/Firewalls	**Commercieel**	**Technisch**	**Switches L2/L3**	**Commercieel**	**Technisch**
Prijs tot 700	V		Prijs tot 500	V	
Binnen 7 dagen leverbaar	V		Binnen 7 dagen leverbaar	V	
Tot aan 50 gebruikers	V	V	24 - 48 poorten	V	V
All-in-one oplossing		V	Web interface		V

Tabel 6 Globale eisen P2 categorie

P3					
Eisen			**Eisen**		
Routers/Firewalls	**Commercieel**	**Technisch**	**Switches L2/L3**	**Commercieel**	**Technisch**
Prijs vanaf 700	V		Prijs vanaf 500	V	
Binnen 7 dagen leverbaar	V		Binnen 7 dagen leverbaar	V	
Tot aan 100 gebruikers	V	V	24 - 48 poorten	V	V
All-in-one oplossing		V	PoE versie beschikbaar		V
			Web interface		V
			Stacking functionaliteit		V

Tabel 7 Globale eisen P3 categorie

5.2 SPECIFIEKE EISEN

D De shortlist bevat een aantal specifieke eisen welke de basis vormen van de productvergelijking. De eisen zijn verkregen via brainstormsessies met de netwerkspecialisten. Vervolgens zijn ze met behulp van deskresearch beschreven en verdeeld over de klantcategorieën. Om het geheel overzichtelijk te houden, zijn de eisen verdeeld over een aantal categorieën die de inhoud van de eis classificeren. Deze onderverdeling bestaat uit vijf verschillende classificaties, namelijk: toekomstvastheid, beheerbaarheid, features, veiligheid en ondersteuning/fabrikant.

Toekomstvastheid
Toekomstvastheid geeft aan hoe lang een bepaald apparaat mee gaat en compatibel blijft met de nieuwste technologieën. Constant IT wil graag apparatuur aan klanten leveren waar lange tijd mee gedaan kan worden. Onder toekomstvastheid vallen zaken als snelheid en uitbreidbaarheid.

Beheerbaarheid
Hieronder vallen de eisen die te maken hebben met het beheer van apparatuur. Het is voor Constant IT belangrijk dat beheer eenvoudig kan verlopen. Door eenvoudig en dus efficiënt te kunnen beheren worden doorlooptijden van incidenten verkort. Zaken als remote toegang, back-ups en het verkrijgen van notificaties met behoeve tot up-time vallen onder beheerbaarheid.

Features
Onder features vallen de technische zaken die een apparaat moet kunnen en hebben een directe invloed op de snelheid, betrouwbaarheid of flexibiliteit van een apparaat. Hoe meer features een apparaat heeft hoe flexibeler deze in te zetten valt.

Veiligheid
Onder veiligheid valt alles wat er voor zorgt om indringers en gevaren buiten te houden maar ook om gebruikers te limiteren in wat ze kunnen op het netwerk.

Ondersteuning & fabrikant
De keuze van de fabrikant heeft gevolgen voor het verloop van het beheer, de garantieregelingen en ondersteuning op producten. Het is voor Constant IT niet wenselijk om de hoogste lijn van support te zijn omdat de kennis mogelijk tekort kan schieten bij complexe issues. Er wordt gezocht naar een fabrikant die ondersteuning kan bieden wanneer het echt nodig is.

Met behulp van de MoSCow-methode zijn de eisen verdeeld in een aantal niveaus, zodat in één oogopslag gezien kan worden hoe belangrijk een eis is.
Hieronder zijn de tabellen met de eisen opgenomen, alsmede hun niveau in de MoSCoW-methode en de klantcategorie waarvoor ze relevant zijn. De MoSCoW-methode kent vier verschillende niveaus:

Figuur 4 MoSCoW

- **Must haves**: Eisen die minimaal aanwezig moeten zijn, zonder deze eisen is een apparaat niet goed genoeg om aan klanten te leveren;
- **Should haves**: Eisen die gewenst zijn. Zonder deze eisen is het product niet onbruikbaar, maar apparatuur dat wel aan deze eisen voldoet is een pre;
- **Could haves**: Deze eisen worden beschouwd als extra en wegen bijna niet mee in de productselectie;
- **Won't haves**: Apparatuur hoeft niet aan deze eisen te voldoen (International Institute of Buisiness Analysis - Pagina 109, 2009).

Voor onderstaande tabellen geldt dat een “V ”aangeeft dat de eis relevant is voor deze klantcategorie. Een “X” geeft aan dat deze eis niet relevant is.

5.2.1 SWITCHES

In de onderstaande tabellen zijn de eisen opgenomen die van toepassing zijn op de switches. Al de onderstaande eisen zijn volledig uitgelegd in paragraaf 3.2 van bijlage drie.

Niveau eisen	Toekomstvastheid	P1 (laag)	P2 (middel)	P3 (hoog)
Must have	• Ipv6	V	V	V
	• Alle poorten minimaal 1Gb	V	V	V
	• Stacking P3*	X	X	V
Should have	• Uitbreidbaarheid (extra poorten)	X	X	V
	• Stackable voor grote klanten	X	X	V
	• Mogelijkheden tot failover	X	V	V
Could have	• Support voor 10GE via koper of fiber	X	X	V
	• Stacking P2*	X	V	X
Won't have				

Tabel 8 Eisen toekomstvastheid - Switches
***Stacking is een could have eis voor P2 maar kan wel meerwaarde bieden. Voor P3 is stacking een must have.**

	Beheerbaarheid	P1 (laag)	P2 (middel)	P3 (hoog)
Must have	• Loggen via webinterface, syslog of mail.	V	V	V
	• Backup en export van configs	V	V	V
	• Remote access via telnet, ssh, web, tool.	V	V	V
Should have	• Notificaties (send mail when down)	X	V	V
	• Console port	X	V	V
	• Reporting op basis van vooraf ingestelde paramaters	X	V	V
	• Diagnostische tools	X	V	V
Could have	• Opties voor centraal beheer	X	V	V
Won't have	• Kaseya integratie	N.V.T	N.V.T	N.V.T

Tabel 9 Eisen beheerbaarheid - Switches

	Features	P1 (laag)	P2 (middel)	P3 (hoog)
Must have	• Etherchannel(LACP)	X	V	V
	• QoS	V	V	V
	• LLDP	X	V	V
	• SNMP	V	V	V
Should have				
Could have	• Power over ethernet (PoE)	V	V	V
Won't have				

Tabel 10 Eisen features - Switches

	Veiligheid	P1 (laag)	P2 (middel)	P3 (hoog)
Must have	• VLAN (en VTP)	V	V	V
Should have	• Security levels instellen	X	V	V
	• ACL	X	X	V
Could have				
Won't have				

Tabel 11 Eisen veiligheid – Switches

	Ondersteuning	P1 (laag)	P2 (middel)	P3 (hoog)
Must have	• Community	V	V	V
	• Helpdesk support	X	V	V
Should have	• Certificering & partnerships	V	V	V
Could have	• Training	X	V	V
Won't have				

Tabel 12 Eisen ondersteuning - Switches

5.2.2 ROUTERS

Deze paragraaf bevat de tabellen waarin de eisen staan die van toepassing zijn op de routers. Al de onderstaande eisen zijn ook uitgelegd in hoofdstuk 3.3 van bijlage 3

	Toekomstvastheid	P1 (laag)	P2 (middel)	P3 (hoog)
Must have	• Mogelijkheid tot clustering	X	X	V
	• Multi wan (failover of bundelen)	V	V	V
	• Gigabit poorten	V	V	V
	• IPv6	V	V	V
	• Link aggregation	X	V	V
Should have				
Could have	• Uitbreidbaarheid via licenties	V	V	V
Won't have				

Tabel 13 Eisen toekomstvastheid – Routers

	Beheerbaarheid	P1 (laag)	P2 (middel)	P3 (hoog)
Must have	• Loggen via webinterface, syslog of mail.	V	V	V
Should have	• Reporting op basis van vooraf ingestelde paramaters	X	V	V
	• Console port aansluiting	X	V	V
	• Diagnostische tools	V	V	V
Could have	• Opties voor centraal beheer	X	X	V
Won't have	• Kaseya integratie	X	X	X

Tabel 14 Eisen beheerbaarheid – Routers

	Features	P1 (laag)	P2 (middel)	P3 (hoog)
Must have	• Site to site VPN	V	V	V
	• Voldoende VPN troughput	V	V	V
	• VPN failover	X	V	V
	• Qos & Traffic management/shaping	V	V	V
	• Policy based traffic management (ACL)	X	X	V
	• DHCP	V	V	V
	• SNMP	V	V	V
	• Verschillende NAT types (specifiek NAT loopback)	V	V	V
Should have	• LDAP/AD integratie	X	V	V
	• Modem functionaliteit	V	V	V
Could have				
Won't have				

Tabel 15 Eisen features - Routers

	Veiligheid	P1 (laag)	P2 (middel)	P3 (hoog)
Must have	• IPsec	X	V	V
	• VLAN support	V	V	V
	• ACL's	X	V	V
Should have	• Proxy support / Web filtering.	X	X	V
	• DDOS herkenning.	X	V	V
Could have	• IDS/IPS	X	V	V
	• Security levels instellen	X	V	V
	• Audit logs	X	V	V
Won't have				

Tabel 16 Eisen veiligheid – Routers

	Ondersteuning	P1 (laag)	P2 (middel)	P3 (hoog)
Must have	• Community	V	V	V
	• Helpdesk support	X	V	V
Should have	• Certificering & partnerships	V	V	V
Could have	• Training	X	V	V
Won't have				

Tabel 17 Eisen ondersteuning – Routers

6 DE ERVARINGEN VAN CONSTANT IT MET DE HUIDIGE PRODUCTEN

Het doel van het project is het standaardiseren van een klein aantal apparaten via een productvergelijking. Echter heeft Constant IT ervaring met veel apparaten wat betekend dat het meest geschikte apparaat misschien al ergens staan.
n dit hoofdstuk worden de resultaten beschreven die de deelvraag '*wat zijn de ervaringen met apparatuur die nu geleverd wordt?' zullen beantwoorden*.
Om de deelvraag te kunnen beantwoorden, is er eerst door middel van een brainstormsessie met de werknemers van de afdelingen Systeembeheer en Sales, een lijst opgesteld met apparaten die momenteel geleverd worden door Constant IT. Deze apparaten zijn in tabel 18 opgenomen:

Routers	Firewalls	Switches L2	Switches L3
Draytek 2130	Watchguard XTM 26	Netgear GS108	Cisco Catalyst 2960
Draytek 2925Vn+	Watchguard XTM 26	Cisco SG200	
	Watchguard XTM33	Cisco SG300	

Tabel 18 Overzicht apparatuur waar men ervaring mee heeft

Er is bewust niet gekozen voor een volledige inventarisatie van alle apparaten, omdat Constant IT als doelstelling heeft om over te stappen naar een kleine selectie apparaten.
Met behulp van open interviews zijn de ervaringen achterhaald die de medewerkers van Constant IT hebben met de met de huidige apparatuur. De resultaten van de interviews worden hieronder beschreven. In bijlage 3 zijn de volledige interviews opgenomen, hierin staat ook een overzicht waarmee gezien kan worden hoe de resultaten verwerkt zijn.

6.1 ROUTERS

Draytek
Over het algemeen hebben de geïnterviewden goede ervaringen met deze apparaten. De Drayteks worden geprezen om hun goede prijs, brede inzetbaarheid en de hoeveelheid features. De negatieve ervaringen hebben voornamelijk te maken met features die niet correct werken, of niet naar wens werken.
De interviews wijzen uit dat 66.4% van de werknemers die ervaring hebben met de producten van Draytek dit als een positieve ervaring beschrijven.

6.2 FIREWALLS

Watchguard
Constant IT levert uitsluitend Watchuard aan haar klanten. De ervaringen hiermee zijn overwegend goed. De apparaten zijn goed inzetbaar als all-in one oplossing bij diverse klanten. Op dit moment hebben meer dan 25 klanten een Watchguard in gebruik Het apparaat is niet perfect en er zijn wel degelijk problemen. Deze problemen ontstaan, vooral op het gebied van de stabiliteit van VPN tunnels Tevens blijkt ook wanneer er zaken fout gaan dat het apparaat voor sommige medewerkers onoverzichtelijk is qua logging
De interviews wijzen uit dat 71.4% van de werknemers die ervaring hebben met de producten van Watchguard, dit als een positieve ervaring beschrijven.

6.3 SWITCHES

Netgear
De unmanaged netgear GS108-serie wordt intern gebruikt om extra netwerkaansluitingen te verkrijgen. De switches blijken zeer stabiel te zijn, waardoor ze aantrekkelijk zijn voor verkoop aan klanten. Dit gebeurt dan ook steeds vaker. De interviews wijzen uit dat 100% van de werknemers die ervaring hebben met deze switches van Netgear, dit als een positieve ervaring beschrijven.

Cisco SG serie
De Cisco switches (SG serie) zijn de meest verkochte beheerbare switches van Constant IT. Deze switches zijn eenvoudig in te stellen en vormen zelden een probleem op het netwerk. De switches voldoen volgens de werknemers goed aan de eisen van de klant, maar de specialisten van Constant IT zouden graag nog iets meer beheermogelijkheden willen zien. De interviews wijzen uit dat 100% van de werknemers die ervaring hebben met de producten van Cisco, dit als een positieve ervaring beschrijven.

Cisco Catalyst
Voor 'layer 3 switches' zijn Cisco Catalysts de enige switches waar intern ervaring mee is. De Catalyst serie van Cisco is zeer bekend maar, zijn bij de klanten van Constant IT vrij zeldzaam. Er zijn niet veel klanten die een switch van dit kaliber nodig hebben. De enkele ervaringen die er zijn met deze switches zijn uitermate positief. Op deze switches kan alles ingesteld worden waardoor ze ideaal zijn vanuit het beheersperspectief. De interviews wijzen uit dat 100% van de werknemers die ervaring hebben met Cisco Catalysts, dit als een positieve ervaring beschrijven. Hierbij moet wel genoemd worden dat er slechts twee personen binnen Constant IT praktijkervaring hadden met deze apparatuur.

Constant IT beschikt over een aantal apparaten welke uitermate interessant zijn voor de productvergelijking door de goede ervaringen. De producten die in tabel 18 staan krijgen dan ook een voorkeursbehandeling.

7 DE UITEENZETTING VAN DE VERGELIJKING

Dit hoofdstuk beschrijft het antwoord op de deelvraag “ Welke eisen wil het management van Constant IT in een beoordelingsmatrix meenemen?.” Het resultaat van de deelvraag is dat Constant IT alle eisen wil meenemen maar niet allemaal even veel laten wegen. Om efficiënt te blijven werken is in overleg met de opdrachtgever besloten geen losse beoordelingsmatrix te maken, maar deze te integreren met de shortlist. Zodoende kunnen alle eisen meetellen maar ook een verschillende weging hebben.
Door de shortlist en de beoordelingsmatrix te integreren met elkaar kan de opdrachtgever in één oogopslag zien welk apparaat voldoet aan welke eisen. Ook valt er in één oogopslag te zien hoe een apparaat zich verhoudt ten opzichte van de concurrentie.

De verschillende apparaten op de shortlist hebben allemaal een totaalaantal aan punten. Dit totaal aantal is gebaseerd op de requirements waaraan zij voldoen. De puntentelling is gebaseerd op de MoSCoW-methode, waarin een onderscheid gemaakt wordt tussen 'must have', 'should have' en 'could have'-eisen. Daarnaast tellen de ervaringen die Constant IT heeft met de apparaten ook mee. De verdelingen van de score is in tabel 19 weergegeven:

Type eis	Waarde
Must have	10 punten
Should have	5 punten
Could have	2 punten
Goede ervaringen Constant IT	20 punten

Tabel 19 Puntenverdeling

8 PRIJS-KWALITEITSVERHOUDINGEN EN SHORTLISTS

De in de eerdere hoofdstukken besproken requirements, ervaringen en verdeling leiden tot de in het dit hoofdstuk besproken shortlists welke het resultaat zijn van de productvergelijking.
In dit hoofdstuk wordt de deelvraag '*wat zijn de prijs-kwaliteitverhoudingen van apparaten die aan de technische wensen voldoen?*' beantwoord. Er wordt inzicht gegeven in de verschillen tussen de aanbevolen apparaten en de niet-aanbevolen apparaten op het gebied features en de prijs-kwaliteitverhouding.

Om tot de best passende producten te komen per klantcategorie zijn er shortlists gemaakt waarmee requirements kunnen worden afgevinkt. Het hele proces is gebaseerd op de methode “Pakketselectie HU”, ontwikkeld door Harry Beerlage (Utrecht, 2013). Er is voor deze methode gekozen, omdat met behulp van de tabellen in één oogopslag gezien kan worden welk apparaat het beste uit de vergelijking komt.
Het aantal requirements vereisten waaraan voldaan wordt, resulteert in een puntenaantal dat leidt tot de prijs-kwaliteitverhouding. Omdat het belangrijk is om te weten hoe de prijs-kwaliteitverhouding tot stand komt, zijn in de hoofstukken hieronder de volledige shortlists meegenomen.

De berekening die gebruikt is om de prijs-kwaliteitverhouding te berekenen, is de volgende: Puntenaantal / Prijs = Prijs-kwaliteitverhouding. Het puntenaantal wordt bepaald door het aantal eisen waaraan een apparaat voldoet, plus eventuele goede ervaringen die Constant IT heeft met een apparaat. Voor de waarde van de eisen wordt verwezen naar hoofdstuk zeven. Hieronder zijn de shortlists per categorie weergegeven. De in het groen aangegeven apparaten zijn de aanbevolen apparaten. Deze zullen in een later hoofdstuk uitgebreider besproken worden.

8.1 SHORTLIST SWITCH P1

		Special Requirements Switches P1							
		Producten							
					3 Netgear ProSafe JGS524				
				2 Linksys LGS124					
			1 Cisco Sg100-24						
	Niveau eisen								
		Toekomstvastheid							
1	Must	Ipv6	V	V	V				
2	Must	Gigabit poorten	V	V	V				
		Beheerbaarheid							
3	Must	Loggen via webinterface, syslog of mail.	X	X	X				
4	Must	Backup en export van configs	X	X	X				
5	Must	Remote access via telnet, ssh, web, tool.	X	X	X				
		Features							
6	Must	QoS	V	V	V				
7	Must	SNMP	X	X	X				
		Veiligheid							
9	Must	VLANs	V	V	V				
		Ondersteuning							
10	Should	Community	V	V	V				
11	Could	Certificering & partnerships	V	V	X				
		Prijs	€140,01	€100,06	€110,01				
		Goede ervaringen Constant IT	X	X	X				
		Punten:	47	47	45				
		Prijs-kwaliteitverhouding	2,97	2,12	2,44				

Tabel 20 Shortlist Switches P1
***Omdat geen van de apparaten beschikt over eisen 3, 4, 5 en 7 is besloten deze niet mee te laten tellen.**

8.2 SHORTLIST ROUTER P1

		Special Requirements –Routers P1							
		Producten							
		5 Linksys EA6900							
		4 Draytek Vigor 2925Vn+							
		3 Draytek Vigor 2130							
		2 Cisco RV320							
		1 Cisco RV110w							
	Niveau eisen								
		Toekomstvastheid							
1	Must	Gigabit poorten	X	V	V	V	V		
2	Must	IPv6	V	V	V	V	V		
3	Could	Uitbreidbaarheid via licenties	X	X	X	X	X		
		Beheerbaarheid							
4	Must	Loggen via webinterface, syslog of mail.	V	V	V	V	V		
5	Should	Diagnostische tools	V	V	V	V	V		
		Features							
6	Must	Site to site VPN	V	V	V	V	X		
7	Must	Voldoende VPN troughput	V	V	V	V	X		
8	Must	VPN failover	X	V	X	V	X		
9	Must	Qos & Traffic management/shaping	V	V	V	V	V		
10	Must	DHCP	V	V	V	V	V		
11	Must	SNMP	V	V	V	V	X		
12	Must	Verschillende NAT types (specifiek NAT loopback)	X	X	X	X	X		
13	Should	Modem functionaliteit	X	X	X	X	X		
		Veiligheid							
14	Must	VLAN support	V	V	V	V	V		
		Ondersteuning							
15	Must	Community	V	V	V	V	X		
16	Should	Certificering & partnerships	V	V	V	V	X		
		Prijs	€53	€174	€84	€194	€160		
		Goede ervaringen Constant IT	X	X	V	V	X		
		Punten:	100	120	110+20	120 +20	70		
		Prijs-kwaliteitverhouding	0,53	1,45	0,64	1,38	2,28		

Tabel 21 Shortlist routers P1

8.3 SHORTLIST SWITCH P2

Special Requirements Switches P2
Producten
4 Netgear Prosafe GSM7224
3 Cisco SG500-28
2 Cisco SG300-28
1 Cisco SG200-26/50

	Niveau eisen								
		Toekomstvastheid							
1	Must	Ipv6	V	V	V	V			
2	Must	Gbit interfaces	V	V	V	V			
3	Should	Mogelijkheden tot failover	V	V	V	V			
4	Could	Stacking	X	X	V	X			
		Beheerbaarheid							
5	Must	Loggen via webinterface, syslog of mail.	V	V	V	V			
6	Must	Backup en export van configs	V	V	V	V			
7	Must	Remote access via telnet, ssh, web, tool.	V	V	V	V			
8	Should	Notificaties (send mail when down)	X	X	X	X			
9	Should	Reporting op basis van vooraf ingestelde paramaters	X	X	X	X			
10	Should	Console Port	X	V	V	V			
11	Should	Diagnostische tools	V	V	V	V			
12	Could	Opties voor centraal beheer	X	X	X	X			
		Features							
13	Must	Etherchannel(LACP)	V	V	V	V			
14	Must	QoS	V	V	V	V			
15	Must	LLDP	V	V	V	V			
16	Must	SNMP	X	V	V	V			
17	Should	Layer 3 functionaliteit	X	V	V	V			
		Veiligheid							
18	Must	VLAN	V	V	V	V			
19	Should	VLAN verspreiding	X	X	V	X			
20	Should	Security levels instellen	X	V	V	X			
21	Should	ACL	X	V	V	V			
		Ondersteuning							
22	Must	Community	V	V	V	V			
23	Must	Helpdesk support	V	V	V	V			
24	Should	Certificering & partnerships	V	V	V	V			
25	Could	Training	V	V	V	V			
		Prijs	€208	€372	€478	€319			
		Prijs per poort	€8	€13	€17	€13			
		Goede ervaringen Constant IT (+20 punten)	V	V	V	X			
		Punten:	132+20	167+20	175+20	165			
		Prijs-kwaliteitverhouding	1,37	2,04	2,45	1,96			

Tabel 22 Shortlist switches P2

8.4 SHORTLIST ROUTER & FIREWALLS P2

			Special Requirements –Routers P2							
			Producten							
		4	Zyxel USG110							
		3	Watchguard XTM26							
		2	Fortigate 40C							
		1	Cisco ASA 5505							
	Niveau eisen									
			Toekomstvastheid							
1	Must		Multi wan (failover of bundelen)	V	V	V	V			
2	Must		Gigabit poorten	X	V	V	V			
3	Must		IPv6	V	V	V	V			
4	Must		Link aggregation	V	V	V	V			
5	Could		Uitbreidbaarheid via licenties	V	V	V	V			
			Beheerbaarheid							
6	Must		Loggen via webinterface, syslog of mail.	V	V	V	V			
7	Should		Reporting op basis van vooraf ingestelde paramaters	V	X	V	X			
8	Should		Console port aansluiting	V	V	V	V			
9	Should		Diagnotische tools	V	X	X	V			
			Features							
10	Must		Site to site VPN	V	V	V	V			
11	Must		Voldoende VPN troughput	V	V	V	V			
12	Must		VPN failover	V	X	V	V			
13	Must		Qos & Traffic management/shaping	V	V	V	V			
14	Must		DHCP	V	V	V	V			
15	Must		SNMP	V	V	V	V			
16	Must		Verschillende NAT types (specifiek NAT loopback)	V	X	V	V			
17	Should		LDAP/AD integratie	V	V	V	V			
18	Should		Modem functionaliteit	X	X	X	X			
			Veiligheid							
19	Must		IPsec	V	V	V	V			
20	Must		VLAN support	V	V	V	V			
21	Must		ACL's	V	V	V	V			
22	Should		DDOS herkenning.	X	X	V	X			
23	Could		IDS/IPS	V	V	V	V			
24	Could		Security levels instellen	V	V	V	V			
25	Could		Audit logs	V	V	V	X			
			Ondersteuning							
26	Must		Community	V	X	V	X			
27	Must		Helpdesk support	V	V	V	V			
28	Should		Certificering & partnerships	V	V	V	V			
29	Could		Training	V	V	V	V			
			Prijs	€595	€500	€500	€486			
			Goede ervaringen Constant IT			V				
			Punten:	203	167	205+ 20	188			
			Prijs-kwaliteitverhouding	2,93	2,99	1,77	2,58			

Tabel 23 Shortlist routers & firewalls P2

8.5 SHORTLIST SWITCH P3

		Special Requirements Switches P3							
		Producten							
		6 HP 2920- 48g							
		5 HP 2910al- 48g							
		Cisco Catalyst 2960X-48TS-L							
		Cisco Catalyst 2960S-48TS-L							
		Cisco SG500X-48							
		1 Cisco SG500-52							
	Niveau eisen								
		Toekomstvastheid							
1	Must	Ipv6	V	V	V	V	V	V	
2	Must	Gbit interfaces	V	V	V	V	V	V	
3	Should	Uitbreidbaarheid (extra poorten)	V	V	V	V	V	V	
4	Should	Mogelijkheden tot failover	V	V	V	V	V	V	
5	Could	Support voor 10GE via koper of fiber	X	V	V	V	V	V	
6	Must	Stacking	V	V	V	V	V	V	
		Beheerbaarheid							
7	Must	Loggen via webinterface, syslog of mail.	V	V	V	V	V	V	
8	Must	Backup en export van configs	V	V	V	V	V	V	
9	Must	Remote access via telnet, ssh, web, tool.	V	V	V	V	V	V	
10	Should	Notificaties (send mail when down)	X	X	X	X	X	X	
12	Should	Console Port	V	V	V	V	V	V	
13	Should	Reporting op basis van vooraf ingestelde paramaters	X	X	V**	V**	X	X	
14	Should	Diagnostische tools	V	V	V	V	V	V	
15	Could	Opties voor centraal beheer	V*	V*	V*	V*	V*	V*	
		Features							
16	Must	Etherchannel(LACP)	V	V	V	V	V	V	
17	Must	QoS	V	V	V	V	V	V	
18	Must	LLDP	V	V	V	V	V	V	
19	Must	SNMP	V	V	V	V	V	V	
20	Should	Layer 3 functionaliteit	V	V	V	V	V	V	
		Veiligheid							
21	Must	VLAN	V	V	V	V	V	V	
22	Must	VLAN verspreiding	V	V	V	V	V	V	
23	Should	Security levels instellen	V	V	V	V	V	V	
24	Should	ACL	V	V	V	V	V	V	
		Ondersteuning							
25	Must	Community	V	V	V	V	V	V	
26	Must	Helpdesk support	V	V	V	V	V	V	
27	Should	Certificering & partnerships	V	V	V	V	V	V	
28	Could	Training	V	V	V	V	V	V	
		Prijs	€775	€1115	€1880	€2078	€2117	€1799	
		Prijs per poort	€15	€23	€39	€43	€44	€37	
		Goede ervaringen Constant IT	V	V	V	V	X	X	
		Punten:	184+20	186+20	191+20	191+20	186	186	
		Prijs-kwaliteitverhouding	3,45	5.41	8,90	10.33	12,02	10,22	

Tabel 24 Shortlist switches P3

*** Een stack van switches kan beheerd worden op één IP, niet alle switches over alle klanten.**

**** Via Cisco IOS Flexible NetFlow (Cisco, 2008).**

8.6 SHORTLIST ROUTER & FIREWALLS P3

		Special Requirements –Routers P3						
		Producten						
		6						
		5 Watchguard XTM5XX (515/525)						
		4 Watchguard XTM330						
		3 Watchguard XTM33						
		2 Fortigate80CM						
		1 Sonicwall NSA 2600						
	Niveau eisen							
		Toekomstvastheid						
1	Must	Mogelijkheid tot clustering	V	V	V	V	V	
2	Must	Multi wan (failover of bundelen)	V	V	V	V	V	
3	Must	Gigabit poorten	V	V	V	V	V	
4	Must	IPv6	V	V	V	V	V	
5	Must	Link aggregation	V	V	V	V	V	
6	Could	Uitbreidbaarheid via licenties	X	V	V	V	V	
		Beheerbaarheid						
7	Must	Loggen via webinterface, syslog of mail.	V	V	V	V	V	
8	Should	Reporting op basis van vooraf ingestelde paramaters	V	V	V	V	V	
9	Should	Console port aansluiting	V	V	X	V	V	
10	Should	Diagnotische tools	V	X	V	V	V	
11	Could	Opties voor centraal beheer	V	V	V	V	V	
		Features						
12	Must	Site to site VPN	V	V	V	V	V	
13	Must	Voldoende VPN troughput	V	V	V	V	V	
14	Must	VPN failover	V	V	V	V	V	
15	Must	Qos & Traffic management/shaping	V	V	V	V	V	
16	Must	Policy based traffic management (ACL)	V	V	V	V	V	
17	Must	DHCP	V	V	V	V	V	
18	Must	SNMP	V	V	V	V	V	
19	Must	Verschillende NAT types (specifiek NAT loopback)	V	X	V	V	V	
20	Should	LDAP/AD integratie	V	V	V	V	V	
21	Should	Modem functionaliteit	X	V	X	X	X	
		Veiligheid						
22	Must	IPsec	V	V	V	V	V	
23	Must	VLAN support	V	V	V	V	V	
24	Must	ACL's	V	V	V	V	V	
25	Should	Proxy support / Web filtering.	V	V	V	V	V	
26	Should	DDOS herkenning.	V	V	V	V	V	
27	Could	IDS/IPS	V	V	V	V	V	
28	Could	Security levels instellen	V	X	V	V	V	
29	Could	Audit logs	V	V	V	V	V	
		Ondersteuning						
30	Must	Community	X	V	V	V	V	
31	Must	Helpdesk support	V	V	V	V	V	
32	Should	Certificering & partnerships	V	V	V	V	V	
33	Could	Training	V	V	V	V	V	
		Prijs	€1810	€1200	€1100	€1400	€2034	
		Goede ervaringen Constant IT			V	V		
		Punten:	225	238	237 +20	239+20	239	
		Prijs-kwaliteitverhouding	8,04	5,04	4,28	5,40	8,51	

Tabel 25 Shortlist routers & firewalls P3

9 DE AANBEVOLEN APPARATEN

Dit hoofdstuk beschrijft de resultaten van het vergelijkend onderzoek dat gedaan is en geeft antwoord op de deelvraag: “welke apparaten zijn het meest passend in de verschillende klantcategorieën?” Alleen de apparaten die als beste uit de vergelijking zijn gekomen worden hier kort beschreven. Er wordt onderbouwd waarom deze apparaten aanbevolen zijn. De resultaten zijn gebaseerd op de shortlists die in het vorige hoofdstuk staan. Het volledige onderzoek is te vinden in de bijlage vergelijkend onderzoek.

9.1 SWITCH P1

Linksys LGS124
Linksys biedt met deze switch een oplossing die voldoet aan de verwachtingen van klanten die weinig eisen stellen aan het apparaat. De switch is *unmanaged* en beschikbaar in uitvoeringen met 16 en 24 poorten. De switch is omringd door een stevig chassis van metaal. Het apparaat beschikt over geavanceerde Quality of Service (QoS) features zodat VoIP verkeer goed werkt en de kwaliteit hiervan gegarandeerd kan worden. De switch beschikt over een hoge doorvoercapaciteit (48Gbps), waardoor er niet snel behoefte zal zijn aan vervanging.

Het onderzoek heeft uitgewezen dat alle switches die getest zijn in deze categorie gelijkwaardig waren, echter viel de Linksys op door de gunstige prijs-kwaliteitverhouding en is deze commercieel gezien daardoor de beste keuze (Linksys / Belkin international, 2013)

Figuur 5 Linksys LGS124

9.2 ROUTER P1

Draytek Vigor 2130
Deze Draytek router onderscheidt zich van de rest van de routers op de markt, doordat het over gigabit WAN- en LAN-poorten beschikt tegen een lage prijs. Daarnaast is er een mogelijkheid om VPN-verbindingen te maken, maar er zijn maar maximaal twee gelijktijdige VPN-verbindingen mogelijk. Dit kunnen twee site-to-site verbindingen zijn, twee site-to-client verbindingen, of een combinatie hiervan. Qua features doet de router niet veel onder voor de Cisco RV320, terwijl laatstgenoemde meer dan twee keer zo duur is (Draytek, n.d.). De Draytek Vigor 2130 wordt aanbevolen omdat de prijs-kwaliteitverhouding deze router onderscheidt van de rest, daarnaast heeft Constant IT al ervaring met dit apparaat. Dit betekent dat eventuele problemen sneller opgelost kunnen worden.

Figuur 6 Draytek Vigor 2130

9.3 SWITCH P2

Cisco SG300
Met de SG serie probeert Cisco de bekende Cisco-kwaliteit te leveren voor een concurrerende prijs. In de productvergelijking zijn zowel de SG200 als de SG300 meegenomen. Deze switches hebben gelijke mogelijkheden op het gebied van layer 2, maar de SG300 kan ook in layer 3-modus gezet worden, waardoor deze veel flexibeler is. Daarnaast is de SG300 ook zeer sterk op het gebied van beheer, omdat deze ook bereikbaar is via telnet en SSH. De SG300 beschikt ook over een console poort, voor het geval dat het apparaat niet op afstand benaderd kan worden.

De prijs-kwaliteitverhouding van de Cisco SG200 is veruit het beste. Toch is voor deze categorie de Cisco SG300 aanbevolen, omdat deze meer compleet is doordat deze beschikt over meer features. Zo kunnen er met de SG300 bijvoorbeeld security levels ingesteld worden per gebruiker, of kan het apparaat als router functioneren met statische routes en access control lists (ACL's). De SG300 voldoet aan bijna alle technische eisen en scoort gelijk aan switches die veel duurder zijn bij de gestelde requirements.

Figuur 7 SG300-3

9.4 ROUTER P2

Watchguard XTM26
Watchguard levert met de XTM26 een all-in-one oplossing met een scherpe prijs. Het licentiemodel van Watchguard is zo opgebouwd dat er een basisapparaat gekocht wordt, wat vervolgens uitgebreid kan worden met allerlei features zoals intrusion prevention systems(IPS), Data loss prevention en (advanced persistent threat blocker (APT blocker). Deze laatste functie kan de "zero day" malware stoppen (Watchguard, 2014). De Watchguard-systemen kunnen gebruikmaken van Watchguard Dimension. Watchguard Dimension is een syslog server die tevens grafisch weergeeft wat er op het apparaat gebeurt. Er kunnen in principe een oneindige hoeveelheid Watchguards aangesloten worden op Dimension, waardoor het een krachtige middel is om alle Watchguards binnen de eigen organisatie in het oog te houden (Watchguard, 2014). Het grootste voordeel van Dimension is dat het gratis is. Op dit moment levert Constant IT al vrijwel exclusief Watchguard firewalls bij klanten. Het onderzoek wijst uit dat dit een zeer goede keuze is, de Watchguard biedt namelijk de meeste features in vergelijking met de andere apparaten.

Figuur 8 Watchguard XTM26

9.5 SWITCH P3

SG500
De SG500 is de high end switch van de Cisco Small and Medium enterprises (SME) serie. De SG500 komt als meest geschikt uit de vergelijking vanwege de prijs-kwaliteitverhouding. De SG500 doet alles wat Constant IT nodig heeft maar mist wel bepaalde features ten opzichte van de andere apparaten. Zo is er bijvoorbeeld geen 10GE module om mee te stacken, de SG500 heeft slechts 5GE modules. Ook is er geen virtual router redundancy protocol (VRRP) protocol aanwezig waarmee meerdere stacks aangemaakt kunnen worden. Echter zijn dit geen 'must have' eisen voor Constant IT en zijn er geen klanten die hiervan gebruik maken. Dit betekent dat de SG500 aan de eisen voldoet tegen de beste prijs, andere switches binnen deze categorie zijn vaak tweemaal duurder.

Figuur 9 SG500

9.6 ROUTER P3

Watchguard XTM330 en 33
De XTM 3 serie is de grotere broer van de eerder genoemde XTM2 serie en bestaat uit twee modellen.
Enerzijds is er de XTM33, een klein apparaat dat geschikt is voor het aansluiten van kleine bedrijven. Anderzijds is er de grote XTM330, een rackmounted apparaat. Qua features verschillen de apparaten inhoudelijk niet, de enige verschillen zijn fysiek. Zo is de XTM330 met snellere hardware uitgerust en wordt deze niet passief gekoeld. De XTM330 is geschikt voor plaatsing in datacentra of op hoofdkantoren, terwijl de XTM33 de verschillende 'branch offices' moet koppelen aan de infrastructuur (Watchguard, 2014).

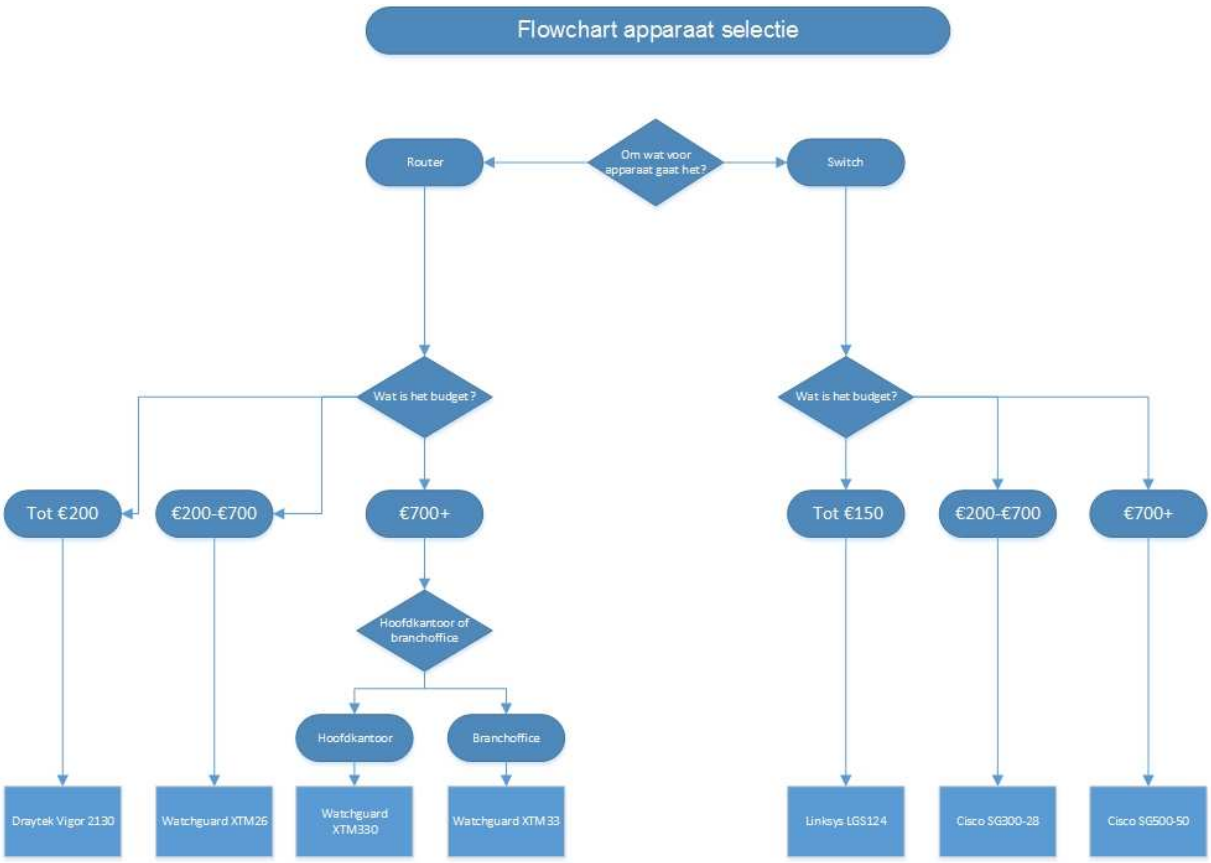
Uit het onderzoek is gebleken dat de Watchguard 3-serie de beste keuze is op basis van de gestelde requirements. Watchguard beveelt aan deze apparaten te combineren zoals hierboven beschreven. De verschillende XTM 33's verbinden allemaal naar het hoofdkantoor waar de XTM330 staat. Alle apparaten in deze categorie liggen dicht bij elkaar op het gebied van de hoeveelheid requirements waaraan voldaan is. Er is echter al veel ervaring met de Watchguards binnen Constant IT, omdat deze al enige tijd geleverd worden. Omdat de andere apparaten niet meer bieden en in sommige gevallen duurder zijn, luidt het advies dat de XTM 3-serie het meest passend is.

Figuur 11 Watchguard XTM33


Figuur 10 Watchguard XTM330

9.7 FLOWCHART

Om de besluitvorming voor sales eenvoudiger en met minder communicatie naar de technische afdelingen mogelijk te maken is een flowchart ontwikkeld op basis van de in het vorige hoofdstuk genoemde resultaten. Deze flowchart bevat een aantal vragen welke uiteindelijk leiden tot één van de aanbevolen producten.



Figuur 12 Flowchart

10 PROOF OF CONCEPT

Dit hoofdstuk beschrijft de resultaten die noodzakelijk zijn om de deelvraag: “Hoe kunnen de resultaten van het theoretisch onderzoek worden getoetst in de praktijk?.” Er is gekozen voor een proof of concept naast het theorie onderzoek omdat het voorkomt dat apparaten in de praktijk minder goed presteren dan geadverteerd. Het proof of concept wordt gedaan om de resultaten van het theoretisch onderzoek te waarborgen. Het proof of concept (PoC) bestaat uit twee delen, deze resultaten hiervan zullen apart benoemd worden na de uitleg van de testopstelling. Alle overige informatie valt te vinden in bijlage 5

10.1 DE TESTOPSTELLING

Er zijn met behulp van Constant IT een aantal apparaten geregeld, waarmee getest kan worden in dit PoC:

- Een Watchguard XTM 26 firewall, die als beste uit de test kwam voor firewalls in de P2-categorie;
- Twee Cisco SG200 switches, die niet als beste uit de test kwamen in de P2-categorie. Deze switches zijn op het gebied van layer 2 functionaliteiten en hardware compleet gelijk aan de wel aanbevolen SG300.
- Een Watchguard XTM 505 firewall, die niet aan tests zal worden onderworpen en alleen gebruikt wordt voor connectiviteit.

Omdat er een aantal tests specifiek voor de aanbevolen Cisco SG300 zijn, worden deze na overleg met de opdrachtgever getest op een SG300 die bij een klant in gebruik is. Deze SG300 functioneert al jaren met de te testen features waardoor ook de stabiliteit te garanderen valt.
De complete omgeving wordt volgens de 'best practices’ opgebouwd die door de fabrikant gesteld zijn. Voor Watchguard firewalls is hiervoor een driedaagse basistraining gevolgd. Deze training is voldoende om alle testgevallen te kunnen uitvoeren. Tevens is er documentatie van Watchguard gebruikt voor de configuratie, deze is gehost op Dropbox.[2] De Cisco switches zijn geconfigureerd op de wijze die beschreven staat in de documentatie op de Cisco website.[3] Daarnaast doet de bedrijfslaptop dienst als client voor het verzenden van data over de infrastructuur, en als logserver voor het ontvangen van berichten van de Watchguard firewall(s).
Meer details over de testopstelling en de procesgang zijn te vinden in hoofdstuk twee van bijlage 5.

Figuur 13 Testopstelling PoC.
Van boven naar onder: Watchguard XTM26, Watchguard XTM505, 2 Cisco SG200-52’s

[2] Watchguard documentatie gehost op Dropbox.com
[3] Cisco documentatie op Cisco.com

10.2 RESULTATEN VAN DE TESTS

In het op TMAP gebaseerde testplan dat in bijlage vijf te vinden is zijn er 37 testpunten gedefinieerd. (Sogeti, 2011)De tests die binnen TMAP 'testgevallen' genoemd worden en voortvloeien uit de testpunten zijn afgeleid van de requirements die gesteld zijn. De testgevallen zijn controleren dus of apparaten wel doen wat er geadverteerd wordt.

	Testcases met OK	Testcases met NOK	Totaal aantal testcases
SG200/SG300	14	2	16
Watchguard XTM26	21	0	21

Tabel 26 Overzicht succesvolle tests

Voor de firewall zijn alle tests met een OK afgerond wat betekend dat deze goed gebruikt kan blijven worden in omgevingen die Constant IT beheert. Voor de switches ligt dit wat lastiger, wij hadden beschikking tot een SG200 terwijl de SG300 was aanbevolen. Gelukkig is er uiteindelijk de mogelijkheid geboden om een SG300 bij een klant te testen. Alle tests waarop de SG200 een OK zou kunnen scoren zijn op de SG200 uitgevoerd. De tests die niet uitgevoerd konden worden zijn uitgevoerd op de SG300, dit zijn de layer 3 tests zoals ACL's en het aanmaken van gebruikers met gelimiteerde toegang. De test hebben bewezen dat er 14 van de 16 tests met een OK beantwoord worden. Het gemis van de laatste twee features (stacking en VTP) is geen probleem voor Constant IT omdat dit geen must have eisen waren voor deze categorie. De twee geteste apparaten (Watchguard XTM26 en Cisco SG300 kunnen beiden succesvol ingezet worden in een klantomgeving).

10.3 RESULTATEN CASUS MALWARE BLOKKEREN

Deze casus is tot stand gekomen nadat een aantal klanten geïnfecteerd zijn met een cryptolocker malware, wat tot veel schade en dataverlies kan lijden. Cryptolocker malware zorgt ervoor dat bestanden op de pc van het slachtoffer met een zeer sterke encryptie worden versleuteld. De gebruiker weet niet wat het wachtwoord is voor het ontsleutelen van de bestanden. De bestanden worden dus als het ware 'gegijzeld'. Vervolgens verschijnen er links naar een website waar betaald kan worden om de sleutel voor de ontgrendeling te verkrijgen (Nachreinier, 2013). Ondanks virusscanners op de lokale computers, worden komen er nog vaak infecties voorbij de scanner. Hierdoor wordt er vaak gezegd door beveiliging specialisten dat alleen een virusscanner niet meer genoeg is (Lastline, 2014). In deze test is de Watchguard firewall ingezet als eerste lijn van verdediging tegen malware.

De casus wijst uit dat met behulp van *subscription services* een zeer goede verdediging met meerdere lagen opgesteld kan worden. De verschillende scans, IPS, Gateway Antivirus, Reputation enabled defense en APT-blocker werken goed samen en vallen eenvoudig in te stellen op de verschillende proxy's die aangemaakt zijn op de firewall om het verkeer te controleren (Watchguard, 2014).
Door de malware testfiles van Eicar te gebruiken, is gebleken dat dreigingen gestopt worden ongeacht of deze via http of https binnen komen, of verstopt zijn in een ZIP-file (Eicar.com, 2014). Zodoende worden dreigingen al gestopt voordat ze bij de computers aankomen.

Door de functionaliteit van de APT-blocker bestaat er ook een bescherming tegen dreigingen die nog niet herkend worden door andere scans, dit zijn de zogenoemde 'zero-day' malware bestanden. De APT-blocker maakt gebruik van cloud functionaliteit om potentiële virussen in een geëmuleerde Windows omgeving uit te voeren. mocht dit een virus zijn dan worden hier definities voor uitgegeven waardoor andere scans dit virus ook kunnen herkennen na een update.
Het heeft zeker een meerwaarde om deze *subscription services* optioneel bij klanten aan te gaan bieden.

11 BUILDING BLOCKS

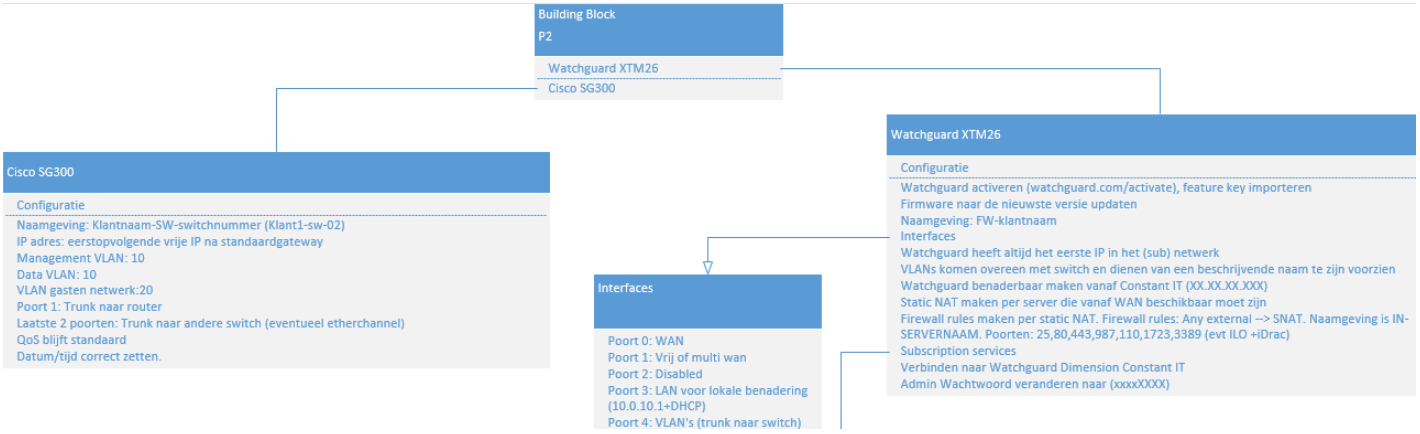
Een building block is een herbruikbaar stuk business, IT of andere architectuur welke individueel een oplossing levert of met andere building blocks gekoppeld kan worden om oplossingen te leveren. De belangrijkste karakteristieken van een building block zijn:

- Een building block is een pakket aan functionaliteit dat in een bepaalde wens voorziet;
- Een building block heeft een duidelijke grens of afbakening;
- Een building block kan samenwerken met andere building blocks;
- Een building block is herbruikbaar, vervangbaar en goed gedocumenteerd.

Voor Constant IT zijn er na afloop van het project ook een aantal building blocks gemaakt, waardoor niet alleen de apparaten gestandaardiseerd worden, maar ook hun configuraties. De building blocks zijn gebaseerd op de verdeling van de klanten. De drie building blocks zijn dus:

- P1: “Klein zakelijk”;
- P2 “MKB”;
- P3 “MKB+”.

De productvergelijking heeft een aantal aanbevolen apparaten opgeleverd welke gestandaardiseerd kunnen worden in een building block. daarnaast is er met behulp van building blocks ook een standaardconfiguratie voor de apparaten beschreven. Door building blocks te gebruiken zullen uiteindelijk het aantal verschillende configuraties bij klanten afnemen. De building blocks zijn terug te zien in figuur 14 en worden in bijlage zes volledig beschreven.



Figuur 14 Building block P2

12 CONCLUSIE

Het doel van het project was om een manier te bedenken om de diversie netwerkconfiguraties bij klanten terug te dringen. Door dit te doen zal er efficiënter gewerkt worden binnen Constant IT.
De hoofdvraag die gesteld was hierbij is: '*Op welke manier kan Constant IT apparatuur bestaande uit switches, routers en firewalls die geadviseerd wordt aan klanten per klantgroep standaardiseren, om de kwaliteit van de dienstverlening op een hoger niveau te krijgen, waarbij van één klantgroep de te standaardiseren apparatuur getest dient te worden?*'
De productvergelijking is na de verdeling tot drie categorieën gelimiteerd.

- P1: “Klein zakelijk”;
- P2: “MKB”;
- P3: “MKB+”.

Uit de productvergelijking zijn 6 apparaten over drie categorieën het meest geschikt bij de gestelde requirements. Hierbij is ook de prijs-kwaliteitverhouding in acht genomen.
Van de P2 klantcategorie (MKB), welke het grootse deel van de klanten vormt is de apparatuur getest in een proof of concept. Het proof of concept wijst uit dat deze apparaten voldoen aan de gestelde tests en dus succesvol kunnen worden ingezet bij klanten.
Daarnaast is er een casus opgesteld voor het inzetten van Watchguard firewalls als eerste lijn van verdediging tegen malware. De testresultaten hiervan staan in bijlage vijf volledig uitgelegd. Echter is er aangetoond dat klanten die voorzien zijn van de Watchguard oplossing tegen malware veel veiliger zijn dan de klanten zonder de malware oplossing van Watchguard.

Om de zes apparaten te standaardiseren zijn deze in een aantal building blocks gezet. Er is één building block per klantcategorie. De building blocks beschrijven ook een standaardconfiguratie, waardoor na verloop van tijd de verschillende klantconfiguraties steeds gelijker worden. Er zullen altijd kleine verschillen blijven bestaan tussen de klantconfiguraties, maar door dezelfde apparaten te gebruiken zal het beheer efficiënter verlopen.

13 AANBEVELINGEN

Op basis van het onderzoek en de conclusies die hieruit getrokken zijn vloeien een aantal aanbevelingen voort
Allereest zullen de overige apparaten die als best uit de productvergelijking kwamen ook getest moeten worden in een proof of concept om hun levensvatbaarheid bij klanten te garanderen. Er is voor deze nog te testen apparaten wel al een building block gemaakt. Het is aan te bevelen om de building blocks en de apparaten die hier in staan te gaan gebruiken bij de verkoop en oplevering van netwerkapparatuur bij klanten. Voor Watchguard firewalls is het aan te bevelen om optioneel een volledige security bundel aan te bieden om de klant infrastructuur te helpen verdedigen tegen malware.
De laatste aanbeveling is dat het onderzoek bij gehouden zal moeten worden. Apparaten die nu het meest geschikt zijn kunnen dat volgend jaar niet meer zijn door veranderende requirements. Daarnaast zouden er nieuwe building blocks kunnen ontstaan doordat Constant IT blijft groeien en andere klanten aan trekt.
De aanbevelingen leiden uiteindelijk tot een lagere diversiteit in netwerkapparatuur bij de klanten, waardoor het beheer voor Constant IT vereenvoudigd wordt. Daarnaast zullen de werknemers meer kennis hebben van de apparaten en kunnen problemen sneller opgelost worden. Door gebruikt te maken van building blocks zal Constant IT efficiënter gaan werken. De building blocks en het onderzoek dat tot de building blocks leidde, zijn zo opgesteld dat deze eenvoudig gewijzigd of uitgebreid kunnen worden met nieuwe categorieën.

OVERZICHT GEBRUIKTE FIGUREN EN TABELLEN

Figuur 1 Organogram Constant IT 12
Figuur 2 Fasering van het project 15
Figuur 3 Verdeling klanten Constant IT 18
Figuur 4 MoSCoW 21
Figuur 5 Linksys LGS124 34
Figuur 6 Draytek Vigor 2130 34
Figuur 7 SG300-3 35
Figuur 8 Watchguard XTM26 35
Figuur 9 SG500 35
Figuur 10 Watchguard XTM330 36
Figuur 11 Watchguard XTM33 36
Figuur 12 Flowchart 37
Figuur 13 Testopstelling PoC. 38

Tabel 1 Producten met goede ervaringen 4
Tabel 2 Puntenverdeling vergelijking 5
Tabel 3 Resultaten onderzoek 5
Tabel 4 Methoden en technieken 17
Tabel 5 Globale eisen P1 categorie 20
Tabel 6 Globale eisen P2 categorie 20
Tabel 7 Globale eisen P3 categorie 20
Tabel 8 Eisen toekomstvastheid - Switches 22
Tabel 9 Eisen beheerbaarheid - Switches 22
Tabel 10 Eisen features - Switches 23
Tabel 11 Eisen veiligheid – Switches 23
Tabel 12 Eisen ondersteuning - Switches 23
Tabel 13 Eisen toekomstvastheid – Routers 24
Tabel 14 Eisen beheerbaarheid – Routers 24
Tabel 15 Eisen features - Routers 25
Tabel 16 Eisen veiligheid – Routers 25
Tabel 17 Eisen ondersteuning – Routers 25
Tabel 18 Overzicht apparatuur waar men ervaring mee heeft 26
Tabel 19 Puntenverdeling 27
Tabel 20 Shortlist Switches P1 28
Tabel 21 Shortlist routers P1 29
Tabel 22 Shortlist switches P2 30
Tabel 23 Shortlist routers & firewalls P2 31
Tabel 24 Shortlist switches P3 32
Tabel 25 Shortlist routers & firewalls P3 33
Tabel 26 Overzicht succesvolle tests 39

BRONVERMELDING

Alani, M. M. (2014). *Guide to OSI & TCP/IP Models.*

Bloomsbury Buisiness Library. (2007). *Bibliotheek HU*. Opgehaald van http://eds.b.ebscohost.com.www.dbproxy.hu.nl/eds/detail/detail?vid=9&sid=86c9aa1f-d2e5-472c-ab90-e445aca8918d%40sessionmgr198&hid=101&bdata=Jmxhbmc9bmwmc2l0ZT1lZHMtbGl2ZQ%3d%3d##db=bsh&AN=26741174

Cisco. (2013). *Cisco SG500(X) productinfo*. Opgehaald van http://www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-500-series-stackable-managed-switches/c22-695647_prod_ov.pdf

Draytek. (sd). *Draytek 2130 productinfo*. Opgehaald van http://www.draytek.nl/files/1-Vigor%202130.pdf

International Institute of Buisiness Analysis - Pagina 109. (2009). *a guide to the business analysis body of knowledge (babok guide)*. Opgehaald van http://www.iowadnr.gov/: http://www.iowadnr.gov/portals/idnr/uploads/Iowa%20Outdoors%20News/2011/BABOK%20Version2.pdf

International Institute of Buisiness Analysis. (2009). *a guide to the business analysis body of knowledge (babok guide)* . Opgehaald van http://www.iowadnr.gov/: http://www.iowadnr.gov/portals/idnr/uploads/Iowa%20Outdoors%20News/2011/BABOK%20Version2.pdf

Investorwords. (sd). *Definition of proof of concept*. Opgehaald van Investorwords: http://www.investorwords.com/3899/proof_of_concept.html

Lastline, G. V. (2014, 5 21). *Antivirus Isn't Dead, It Just Can't Keep Up*. Opgehaald van Labs.lastline.com: http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up

Linksys / Belkin international. (2013). *LGS124 productinfo*. Opgehaald van http://downloads.linksys.com/downloads/datasheet/25820_Belkin_Linksys_Unmanaged_Switches_16_24_Port_PROD.pdf

Nachreinier, C. (2013). *Everything you wanted to knkow about cryptolocker*. Opgehaald van Watchguardsecuitycenter.com: http://Watchguardsecuritycenter.com/2013/11/04/everything-you-wanted-to-know-about-cryptolocker/

Open Group (Building Blocks). (2011). *TOGAF Overview*, 9.1. Opgehaald van www.opengroup.com: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap37.html

Open Group (Introduction to TOGAF). (2011). *Introduction to TOGAF*. Opgehaald van Opengroup.com: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap01.html

Sogeti. (2011). *TMap next*. Opgehaald van TMap: http://www.tmap.net/tmap

Steehouder, M. (2012). *Leren Comminuceren* (Vol. 2). Groningen/Houten: Noordhoff Uitgevers B.V.

Utrecht, H. B. (2013). Pakketselectie van de HU. Utrecht.

Watchguard. (2014). *UTM security modules*. Opgehaald van http://Watchguard.com/wgrd-products/utm/overview/#utm-security-modules

Watchguard. (2014). *Watchguard APT-blocker module*. Opgehaald van Watchguard.com: http://Watchguard.com/wgrd-products/security-modules/apt-blocker

Watchguard. (2014). *Watchguard XTM26 productinfo*. Opgehaald van http://Watchguard.com/docs/datasheet/wg_xtm2_ds.pdf

Watchguard. (2014). *Watchguard XTM3 series productinfo*. Opgehaald van http://www.Watchguard.com/docs/datasheet/wg_xtm3_ds.pdf

Plan van aanpak

Constant IT

26 augustus 2014, Chris de Keijzer
Opleiding: System & Network engineering
Studentnummer: 1591134
Telefoonnummer: 06-10181296
Bedrijf: Constant IT
Versie: 1.0

Constant IT

VERSIEBEHEER

Documentgegevens	
Project titel	Plan van aanpak standaardisering Constant IT
Projectnummer	1.0
Versie	V1.0
Versie datum	9-10-2014
Status	Concept

Opsteller	
Naam	Rol
Chris de Keijzer	Auteur & eindredacteur

Verspreiding		Versie											
Naam	Rol	0.1	0.11	0.12	0.13	0.14	0.15	0.2	0.21	0.22	0.23	1.0	1.1
Allard Borgart	Bedrijfsbegeleider		X	X						X		X	X
Chris Leicher	Docentbegeleider	X		X	X	X	X	X	X	X	X	X	X
Bas de Zeeuw	Technisch begeleider		X	X						X			

INHOUDSOPGAVE

Versiebeheer 2
Inhoudsopgave 3
Verklarende woordenlijst 4
1 Inleiding 5
2 Constant IT 5
3 De aanleiding 6
4 Doelstelling 6
5 De onderzoeksvragen 7
6 Randvoorwaarden en afbakening 7
7 Gebruikte methoden en literatuur 8
7.1 Uitleg methoden en technieken 10
8 Producten en kwaliteitsbewaking 12
9 Fasering 13
9.1 Fase 1 - Voorbereiding 13
9.2 Fase 2 - Inventariseren 13
9.3 Fase 3 - Vergelijkend onderzoek 14
9.4 Fase 4 - Ontwerp & advies 14
9.5 Fase 5 - Proof of concept en afronding 15
9.6 Overzicht projectflow. 16
9.7 Planning 17
10 De plaats in de Organisatie 20
11 Risico's 21
12 De projectorganisatie 22
12.1 De opdrachtgever 22
12.2 De opdrachtnemer 22
12.3 Docentbegeleider 22
12.4 Overige partijen 22
13 De bedrijfs-/persoonsgegevens 23
Referenties 24
Bijlage 25
De opdracht zoals opgeleverd door Constant IT 25
Concept indeling scriptie 26
Contract afstudeeropdracht 27

VERKLARENDE WOORDENLIJST

Apparaat	-	Geleverde hardware, dit is een switch, router of firewall.
Building block	-	Een pakket dat een bepaalde functionaliteit bevat. De kenmerken zijn dat building blocks interoperationeel, herbruikbaar en duidelijk gespecificeerd zijn.
Enterprise Architecture	-	Een blauwdruk die de structuur en organisatie van een bedrijf bepaalt.
Longlist		Een lijst met producten die voldoen aan requirements.
MoSCoW	-	Methode waarmee prioriteiten gesteld kunnen worden.
Premium reseller	-	Verkoper die een band aan gaat met een fabrikant in ruil voor voordelen.
Prijs kwaliteitverhouding		Een waarde toekenning van een product gedeeld door de prijs.
Requirements	-	Eisen.
Shortlist		Een lijst met apparaten die aan eisen en wensen voldoen en waar eventueel goede ervaringen mee zijn. Deze voorkeurslijst is gebaseerd op de longlist
TOGAF	-	Een framework voor Enterprise Architecture.
TMap	-	Methode van gestructureerd testen.

1 INLEIDING

Dit plan van aanpak is geschreven voor Constant IT en Hogeschool Utrecht, het is onderdeel van het afstudeerproject dat uitgevoerd wordt door Chris de Keijzer. Dit document beschrijft de context waarbinnen het afstudeerproject zal plaatsvinden, de aanleiding tot de opdracht en de middelen om de beoogde doelstellingen te bereiken.

2 CONSTANT IT

Constant IT voorziet het midden-en klein bedrijf van systeembeheer services in de omgeving van Amsterdam en heeft een diverse klantenkring met klanten in onder andere de financiële sector en de horeca. Het dienstenpakket bestaat naast systeembeheer op locatie en afstand ook uit verschillende web-diensten en cloud diensten.
Het Constant IT team bestaat uit 18 medewerkers in diverse lagen van de organisatie en groeit snel. Het team beheert de infrastructuur van ongeveer 200 klanten die variëren van kleine eenmanszaken tot bedrijven van ongeveer 200 medewerkers. Omdat het bedrijf steeds groter wordt beogen ze ook om efficiënter te werken en de organisatie volwassener te maken

- Constant IT voorziet zijn klanten van de volgende diensten;
- Systeembeheer (particulier en zakelijk);
- Consultancy en Auditing;
- Cloud diensten zoals hosted exchange, desktop online, online back-up en VoIP;
- Webhosting.

Constant IT levert systeembeheerdiensten op apparatuur die gekocht wordt door de klanten. Bij de aankoop van apparatuur begeleidt Constant IT de klant door het gehele verkooptraject, er wordt advies gegeven en wanneer er een besluit genomen is voorziet Constant IT ook in de levering, configuratie en het beheer.

3 DE AANLEIDING

Constant IT is over de jaren heen snel gegroeid, er zijn meer klanten, meer werknemers en meer diensten. Er worden projecten uitgevoerd die de infrastructuur van klanten aanpast of volledig opnieuw opbouwt. Echter, blijkt nu dat het beheer van geleverde apparatuur bij verschillende klanten steeds complexer wordt door het gebrek aan standaarden. Door beperkte kennis van het volledige assortiment aan apparaten ontstaan de volgende problemen op de technische- en sales afdelingen.

- Elk apparaat kan in potentie een ander probleem krijgen waardoor er incidenten ontstaan;
- Het is onmogelijk om voor elk apparaat technische documentatie te onderhouden;
- Het is onduidelijk welk apparaat bij een klant staat;
- Inwerken van nieuwe collega's vergt meer tijd door de diverse configuraties bij de klanten;
- Besluitvorming vanuit de sales afdeling verloopt traag;
- Het is lastig om passend advies geven op basis van prijs-kwaliteitverhouding en requirements van de klant.

Constant IT wil graag efficiënter gaan werken en daarom willen ze mogelijkheden verkennen met betrekking tot het leveren van standaardoplossingen. Om de wildgroei van apparatuur tegen te gaan. In de visie van Constant IT zou er, met behulp van standaardisatie, een kleine selectie apparaten over blijven die geleverd wordt aan klanten.

4 DOELSTELLING

In dit hoofdstuk wordt de doelstelling van het afstudeerproject beschreven. Bijlage één bevat de opdracht zoals deze opgeleverd is aan de afstudeerder nadat de stageperiode overeen gekomen is. Door verandering van inzichten zijn de doelstellingen van de opdracht enigszins aangepast maar de kern blijft hetzelfde.
Dit afstudeerproject heeft als hoofddoel om de kwaliteit van de dienstverlening te verhogen, het beheer te vereenvoudigen en kostenverlaging tot stand te brengen door het aanbieden van standaarddienstverlening. De kwaliteit van dienstverlening bestaat volgens Constant IT uit:

- Het aantal incidenten;
- De doorlooptijd van incidenten;
- De doorlooptijd van verkooptrajecten;
- De stabiliteit en performance van apparatuur bij klanten;
- Oplossingen aanbieden die aansluiten bij de huidige en toekomstige requirements van de klant.

Dit vergelijkende afstudeerproject met alle ondersteunende elementen die in latere hoofdstukken beschreven worden zullen uiteindelijk leiden tot efficiënter werken en alle daarbij komende voordelen zoals:

- Sneller en efficiënter werken op de afdelingen die geraakt worden door dit afstudeerproject;
- Werknemers hebben diepgaande kennis van een kleine selectie apparaten wat de doorlooptijd van incidenten verkort en de klanttevredenheid ten goede komt;
- Het opzetten van een knowledge base voor een klein aantal apparaten kost minder tijd;
- Het wordt eenvoudiger om interne kennisoverdracht te laten plaatsvinden.

De doelen worden behaald aan de hand van productvergelijkingen en praktijktests van apparaten die vervolgens gestandaardiseerd worden in de vorm van een building block (TOGAF)
Uiteindelijk zal de standaardisatie leiden tot een consistent en voorspelbaar proces met betrouwbare resultaten op de gebieden van beheer en verkoop.
Het minimaal aanwezige om de afstudeeropdracht geslaagd te mogen noemen zijn een productvergelijking die voorziet in richtlijnen met behoeve tot advies en een proof of concept van de apparaten die als beste uit de vergelijking komen.

5 DE ONDERZOEKSVRAGEN

Hoofdvraag

Op welke manier kan Constant IT apparatuur bestaande uit switches, routers en firewalls die geadviseerd wordt aan klanten per klantgroep standaardiseren, om de kwaliteit van de dienstverlening op een hoger niveau te krijgen, waarbij van één klantgroep de te standaardiseren apparatuur getest dient te worden?

Deelvragen

8. Wat zijn de ervaringen met apparatuur die nu geleverd wordt?
9. Hoe zou het management van Constant IT de bestaande klanten willen indelen in categorieën.
10. Welke technische en commerciële eisen en wensen worden er gesteld aan apparatuur door Constant IT en haar klanten, en welke waarde hebben deze?
11. Welke eisen wil het management van Constant IT in een beoordelingsmatrix meenemen?
12. Welke apparaten zijn het meest passend in de verschillende klantcategorieën?
13. Wat zijn de prijs/kwaliteit verhoudingen van apparaten die aan de technische en commerciële wensen voldoen?
14. Hoe kunnen de resultaten van het theoretisch onderzoek worden getoetst in de praktijk?

6 RANDVOORWAARDEN EN AFBAKENING

De randvoorwaarden worden bewaakt door de afstudeerder, de docentbegeleider en bedrijfsbegeleider van Constant IT.

Algemeen

- Dit afstudeerproject heeft geen afhankelijkheden van interne projecten;
- Alle apparaten die worden getest in een proof of concept worden getest met een gratis leenapparaat van de fabrikant;
- De afstudeerder heeft de medewerking van Constant IT nodig.

Binnen de scope

- In kaart brengen van de ervaringen van Constant IT met apparatuur die geleverd wordt;
- Requirements achterhalen via interviews;
- Een productvergelijking opstellen met longlist en shortlist;
- Requirements verwerken in een beoordelingsmatrix;
- Een proof of concept uitgevoerd door de afstudeerder;
- Het proof of concept opzetten volgens door de fabrikant opgestelde “best practices” met apparaten die als beste uit de productvergelijking komen;
- Het proof of concept zal één building block omvatten. Een building block omvat een switch en een router/firewall;
- Het proof of concept wordt getoetst aan de hand van de requirements van Constant IT en de specificaties van de fabrikant;
- Dit afstudeerproject limiteert zich tot switches op layer 2 en 3, routers en dedicated firewalls;
- Maken van op TOGAF gebaseerde building blocks.

Buiten de scope

- Er worden geen klanten geïnterviewd;
- Dit afstudeerproject zal geen draadloze apparaten omvatten;
- Dit afstudeerproject omvat geen softwarematige oplossingen (zoals bijvoorbeeld firewalls op basis van OpenBSD);
- Er vindt bij dit afstudeerproject geen migratie en/of vervanging van apparatuur bij klanten plaats;

- Requirements waarbij blijkt dat er meerdere apparaten van hetzelfde type nodig zijn worden niet getest;
- Toetsen of de kennis van de technische medewerkers over apparaten voldoende is;
- Apparaten die niet bij “preffered partners” te verkrijgen zijn vallen af.

7 GEBRUIKTE METHODEN EN LITERATUUR

Hieronder een methoden matrix met deelvragen en bijhorende methoden

Deelvraag/taak	Methode	Type deelvraag	Resultaat	Doelstelling
Wat zijn de ervaringen met apparatuur die nu geleverd wordt?	Inventarisatie via deskresearch en interviews.	Beschrijvend	Een lijst met apparaten of merken die ervaren worden als “goed” door de medewerkers van Constant IT.	Deze apparaten worden meegenomen in de vergelijking en krijgen bonuspunten. De inventarisatie zal deel uitmaken van een document dat requirements bevat.
Hoe zou het management van Constant IT de bestaande klanten willen indelen in categorieën?	Interviews.	Definiërend	Een verdeling van klanten ten behoeve van productadvies. .	Het vast stellen welke klant groepen er zijn zodat er een basis is voor de productvergelijking.
Welke technische en commerciële eisen en wensen worden er gesteld aan apparatuur door Constant IT en haar klanten, en welke waarde hebben deze?	Desk-research, Interviews.	Verklarend	Een lijst van eisen die zowel technisch als functioneel van aard kunnen zijn om de producten te kunnen scoren. Deze tezamen vormen de “requirements”	De eisen en wensen geven aan waar de te vergelijken apparaten aan moeten voldoen om overwogen te worden. Deze “requirements” vormen de basis van het onderzoek.
Welke eisen wil het management van Constant IT in een beoordelingsmatrix meenemen?	Interview, MoSCow + requirement prioritziation.	Beschrijvend	Een door Constant IT goedgekeurde eisenlijst.	Door overleg te hebben met Constant IT en de te gebruiken requirements te accorderen kan er geen verwarring ontstaan over het beoogde resultaat van het onderzoek.
Welke apparaten zijn het meest passend in de verschillende klantcategorieën?	Pakketselectie HU, Longlist, Shortlist, beoordelingsmatrix, Prijs/Kwaliteitverhouding.	Vergelijkend	De productselectie levert een aantal apparaten op die het best passen bij de gestelde requirements.	Het achterhalen van de beste apparaten zodat deze getest en gestandaardiseerd kunnen worden.
Wat zijn de prijs/kwaliteit verhoudingen van apparaten die aan de technische en commerciële wensen voldoen?	Desk research, gecombineerd met eerder vastgestelde eisen die via MoSCoW een waarde hebben gekregen	Vergelijkend	Een lijst met prijs kwaliteitverhoudingen van apparaten die op de shortlist staan.	Door de prijs/kwaliteit verhouding in kaart te brengen van apparaten op de shortlist wordt duidelijk welk apparaat aan de meeste requirements voldoet voor het minste geld.

Hoe kunnen de resultaten van het theoretisch onderzoek worden getoetst in de praktijk?	Een Proof of concept ondersteund door functioneel en technisch ontwerp	Ontwerpend /evaluerend	Een proof of concept opbouwen waarmee de technische werking van de “beste” apparaten aantoont.	Het proof of concept levert resultaten op waarmee Constant IT besluiten kan gefundeerde besluiten kan maken.
Samenstellen building block.	TOGAF (Alleen building blocks)		De producten die als beste uit de selectie komen worden in een building block gezet. Dit building block komt overeen met de eerder gemaakte onderverdeling van klanten.	Eerder zijn de klanten onderverdeeld in categorieën. Hierop zijn de building blocks gebaseerd. Er kunnen bijvoorbeeld building blocks ontstaan zoals “klant_groot, klant_klein”. De building blocks maken het geheel overzichtelijker.
Planning	Gantt chart		Er komt een overzichtelijke planning waarmee in zowel de fasering als de verschillende einddatums in beeld gebracht worden.	De Gantt chart voorziet in tijdsbewakingen het inzichtelijk maken van taken.
Testplan	TMap		Er wordt een testplan opgesteld dat voorziet in de wijze waarop getest wordt. Het testplan is gebaseerd op de requirements.	Het testplan zorgt er voor dat het testen op een consistente en systematische wijze verloopt.
Proof of concept	Functioneel en technisch ontwerp.		De ontwerpen worden gebaseerd op wat dat als de fabrikant wordt aangedragen als “best practice”.	Door ontwerpen van te voren uit te denken wordt er tijd bespaard in de uitvoerende fase.
Proof of concept	Testplan		Het testplan voorziet in de wijze waarop getest dient te worden en ondersteund het proof of concept.	Door volgens een vaste methode te testen worden er betrouwbare resultaten neergezet waarmee conclusies getrokken kunnen worden.
Sales op de hoogte stellen van verandering van werkwijze	Flowchart		De flowchart voorziet sales van instructies bij aan te schaffen hardware.	Met behulp van een flowchart kan besluitvorming bij sales met minder communicatie naar de technische dienst verlopen.

Tabel 27 Methoden tabel

7.1 UITLEG METHODEN EN TECHNIEKEN

Deskresearch
Deskresearch is de algemene term voor het uitvoeren van literatuuronderzoek of internet research. Binnen het afstudeerproject zal dit regelmatig gebruikt worden omdat fabrikanten van apparaten informatie veelal online hebben staan. Informatie waarnaar gezocht zal worden zijn technische documentatie van apparatuur.

Inventarisatie
Met behulp van een inventarisatie kan in kaart gebracht worden wat Constant IT op dit moment heeft staan qua apparatuur bij de verschillende klanten. Dit wordt in kaart gebracht met behulp van het intern gebruikte monitoringsysteem dat Kaseya heet.

Interviews
Interviewen is een methode om een grote hoeveelheid informatie te achterhalen. Binnen dit afstudeerproject worden de interviews gebruikt om de kennis van Constant IT te gebruiken voor het achterhalen van eisen en wensen. Deze kwalitatieve interviews zullen gedaan worden met sleutelpersonen binnen de organisatie van Constant IT. Het doel van de eerste interviews is het in kaart brengen van de ervaringen en kennisniveaus van apparaten die door Constant IT geleverd worden. Daarnaast zullen interviews ook voorzien in de mogelijkheid een terugkoppelmoment te hebben met de opdrachtgever. Naast interviews die zich concentreren op de eisen en wensen zijn er ook interviews die om de ervaringen draaien die constant IT heeft met apparaten die al in beheer zijn. Apparaten die al in gebruik zijn bij Constant IT en worden ervaren door de medewerkers van Constant IT als goed krijgen bonuspunten in de beoordeling.
De interviews zullen bestaan uit open vragen en worden uitgevoerd zoals beschreven in Leren communiceren van Michael Steehouder (Steehouder, 2012).

TOGAF(building blocks)
TOGAF (The Open Group Architecture Framework) is een kader dat gebruikt wordt om Enterprise Architecture te ontwikkelen. Enterprise Architecture wordt gebruikt om de “enterprise” ofwel het bedrijf te optimaliseren (Open Group (Introduction to TOGAF), 2011). Deze optimalisatie houdt in dat processen die los staan van elkaar Geïntegreerd worden in één geheel waardoor een aantal voordelen ontstaan, waaronder:

- Een efficiëntere bedrijfsvoering;
- Een efficiëntere IT operatie;
- Minder complexiteit in het bedrijf en de IT.

Dit afstudeerproject maakt echter alleen gebruik van het building blocks concept dat in TOGAF zit. De building blocks zijn bouwstenen die op elkaar passen om tot een totaalproduct te komen.
Nadat de klanten in de eerste fase worden verdeeld in categorieën verschijnt er een duidelijke scheiding van de klanten. Hierdoor kunnen de building blocks van TOGAF gekoppeld worden aan een klantcategorie. Het einderesultaat zijn een aantal building blocks die weergeven welk apparaat het beste bij een klantcategorie past. Een goede opzet van building blocks leidt tot verbeteringen op het gebied van integratie, flexibiliteit en efficiëntie bij Constant IT. In de TOGAF methode wordt er zeer veel vrijheid gegeven om een eigen invulling te geven aan de inhoud van de building blocks waardoor dit concept ook na dit afstudeerproject nog gebruikt kan worden. (Open Group (Building Blocks), 2011)

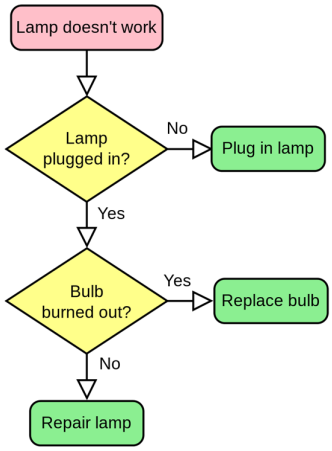
Moscow + requirement prioritization
De MoSCow analyse wordt al jaren gebruikt om op een eenvoudige en betrouwbare wijze eisen en wensen in kaart te brengen. Het doel van de MoSCoW analyse is het in kaart brengen van de “must-have”, “should-have, “could have” en “won’t have” delen van een project. Binnen dit afstudeerproject zal de methode gebruikt worden om de via de interviews verzamelde eisen en wensen te sorteren. Uiteindelijk zal er aan deze eisen en wensen een numerieke waarde worden toegewezen zodat deze in de beoordelingsmatrix passen en een duidelijk resultaat weergeven
Hoe MoSCoW gebruikt moet worden valt te vinden op pagina 102 van: (International Institute of Buisiness Analysis, 2009)

Figuur 15 MoSCoW

Productvergelijking (Pakketselectie HU)
Pakketselecties worden gebruikt om de best passende pakketten te achterhalen door ze tegen de eisen en wensen te houden. In dit afstudeerproject zal ook een pakketselectie uitgevoerd worden om de best passende apparaten te vinden. Echter wordt binnen het afstudeerproject de term productvergelijking gehanteerd. Pakketselecties zijn aan bod gekomen tijdens de lessen van Harry Beerlage, de tabellen die gebruikt worden in de vergelijking zullen ook zoveel mogelijk hetzelfde format aanhouden. (onderzoeksmethoden) (Utrecht, 2013).

Beoordelingsmatrix
Een beoordelingsmatrix wordt gebruikt wanneer er gekozen moet worden tussen meerdere opties, terwijl er wel veel factoren zijn waar rekening mee gehouden moeten worden. Met deze techniek worden alle op de shortlist staande apparaten in een tabel gezet samen met de eisen. Alle eisen hebben een numerieke waarde en het apparaat met de meeste punten is het best passende apparaat.
Prijs kwaliteitverhouding
Constant IT richt zich meestal op producten die de beste prijs kwaliteitverhoudingen hebben, zo blijven de kosten voor Constant IT en hun klanten laag en worden er toch technische sterke producten geleverd. . De prijs kwaliteitverhouding is ook belangrijk in dit afstudeerproject en is een belangrijk deel van de vergelijking. De verhouding zal aanwezig zijn in de beoordelingsmatrix en is gebaseerd op het puntenaantal dat verkregen is door het voldoen aan het aantal eisen gedeeld door de prijs.
Proof of concept
Een Proof of concept wordt gebruikt om van een idee de technische werking aan te tonen in een compacte testomgeving. In de proof of concept van dit afstudeerproject zullen de apparaten getest worden die als beste uit de productvergelijking komen. De zaken die getest worden omvatten het nagaan of de specificaties van de fabrikant kloppen en het testen van configuraties volgens “best practices” zoals gesteld door de fabrikant.(Investorwords, sd)
Functioneel ontwerp & technisch ontwerp
Het functioneel en technisch ontwerp zijn de blauwdrukken van het proof of concept. Het functioneel ontwerp geeft aan hoe de infrastructuur werkt op een wijze dat het ook voor niet technische collega’s te begrijpen is. In het technisch ontwerp wordt het onderliggende technische element besproken, er wordt gericht op het zichtbaar maken van de verschillende technieken en protocollen zodat deze goed over te dragen zijn aan collega’s. De ontwerpen worden opgezet volgens “best practices” van de fabrikant om de optimale werking te garanderen.
Testplan
Een testplan wordt gebruikt om volgens een vaste methode te testen wat resulteert in consistente resultaten. Op basis van consistente testresultaten kunnen goed onderbouwde conclusies worden getrokken. Het testplan is gebaseerd op de TMap methode.
TMap
TMap is een methode die ontwikkeld is voor het consistent en systematisch testen van IT producten Er wordt voor dit afstudeerproject een testplan gemaakt waarin gedefinieerd wordt wat er getest wordt en hoe.(Sogeti, 2011)
Gantt chart
Gantt charts worden gebruikt om een visuele weergave te geven van een planning, er kunnen afhankelijkheden worden laten zien en deadlines worden inzichtelijk gemaakt**.** Deze methode van planning wordt al sinds de 19de eeuw gebruikt. De gantt chart voor dit afstudeerproject valt te vinden in hoofdstuk 9.1 (Bloomsbury Buisiness Library, 2007)

Flowchart
Een flowchart maakt het verloop van procedures inzichtelijk. Voor het afstudeerproject zal een flowchart worden gebruikt om de besluitvorming bij de sales afdeling te versnellen. Door de flowchart te volgen zal er minder communicatie naar de technische afdeling zijn.



Figuur 16 Flowchart voorbeeld

8 PRODUCTEN EN KWALITEITSBEWAKING

Er zijn een aantal producten op te leveren aan Constant IT, te weten:

- Plan van aanpak;
- Requirements document met onderverdeling klanten en resultaten interviews;
- Productvergelijking ondersteund door longlist, shortlist en beoordelingsmatrix;
- Functioneel en technisch ontwerp ten behoeve van proof of concept;
- Testplan, proof of concept en testdocumentatie;
- Adviesrapport met daarin de conclusies van bovenstaande producten;
- Flowchart op basis van resultaten adviesrapport.

Het plan van aanpak dient door alle partijen van een akkoord te worden voorzien. Daarnaast is er voor de overige producten vast gesteld dat Constant IT hiervoor ook akkoord moet geven.
De kwaliteit wordt bewaakt door middel van vergaderingen met de bedrijfsbegeleider die elke week gehouden worden. Er is ook een technisch begeleider aangewezen die ondersteuning biedt bij zowel de school documentatie als de inhoudelijke zaken.
Daarnaast zijn er nog een aantal producten op te leveren aan Hogeschool Utrecht, dit zijn:

- Plan van aanpak;
- Scriptie;
- Presentatie;
- Evaluatie.

De kwaliteit hiervan wordt bewaakt door middel van wekelijkse rapportages aan de docentbegeleider, wanneer er documentatie is gemaakt zal er om feedback gevraagd worden.

9 FASERING

Dit afstudeerproject werkt volgens de watervalmethode waardoor alle stappen sequentieel verlopen.

9.1 FASE 1 - VOORBEREIDING

Uitleg fase 1
In deze fase wordt:

- Er onderzoek gedaan naar TOGAF;
- Het plan van aanpak gemaakt.

Op te leveren (sub)producten

- Plan van Aanpak.

9.2 FASE 2 - INVENTARISEREN

Uitleg fase 2
In deze fase wordt:

- Er een onderverdeling gemaakt van klanten in overleg met Constant IT;
- Geïnventariseerd welke apparaten er op dit moment in beheer zijn;
- Interviews opgesteld en afgenomen;
- Er requirements in kaart gebracht en waarden toegekend aan deze requirements via MoSCoW in overleg met Constant IT.

Op te leveren (sub)producten

- Interview + uitwerkingen;
- Requirements document waarin ook de interviews verwerkt zijn.

Te beantwoorden deelvragen

- Wat zijn de ervaringen met apparatuur die nu geleverd wordt?
- Hoe zou het management van Constant IT de bestaande klanten willen indelen in categorieën.
- Welke technische en commerciële eisen en wensen worden er gesteld aan apparatuur door Constant IT en haar klanten, en welke waarde hebben deze?
- Welke eisen wil het management van Constant IT in een beoordelingsmatrix meenemen?

9.3 FASE 3 - VERGELIJKEND ONDERZOEK

Uitleg fase 3

In deze fase wordt:

- Informatie vergaard over apparaten en hun features;
- Een longlist per categorie opgesteld met apparaten die voldoen aan de basis requirements;
- Een shortlist per categorie opgesteld met door apparaten tegen specifieke requirements af te strepen;
- Een prijs-kwaliteitsverhouding gemaakt van apparaten op de shortlist;
- Een beoordelingsmatrix gemaakt waarmee het meest passende apparaat gevonden wordt per categorie.

Op te leveren (sub)producten

- Longlist;
- Shortlist;
- Productvergelijking.

Te beantwoorden deelvragen

- Welke apparaten zijn het meest passend in de verschillende klantcategorieën?
- Wat zijn de prijs/kwaliteit verhoudingen van apparaten die aan de technische en commerciële wensen voldoen?

9.4 FASE 4 - ONTWERP & ADVIES

Uitleg fase 4
In deze fase wordt:

- Een testplan gemaakt;
- Een functioneel ontwerp gemaakt;
- Een technisch ontwerp gemaakt;
- Er leenapparatuur aangevraagd ten behoeve van het proof of concept.

Op te leveren (sub)producten

- Startdocumentatie van proof of concept omgeving met functioneel ontwerp, technisch ontwerp en testplan;
- Adviesrapport (exclusief testrapportage);
- Flowchart maken voor sales afdeling.

9.5 FASE 5 - PROOF OF CONCEPT EN AFRONDING

Uitleg fase 5
In deze fase wordt:

- Een Proof of concept uitgevoerd met de “beste” apparaten;
- Testresultaten van het proof of concept beschreven de testresultaten tegenover de eisen gezet worden;
- Een advies gegeven over welke apparaten het best in het building block gezet kunnen worden en dus gebruikt worden voor de standaardisatie;
- Een flowchart gemaakt;
- Informatie overgedragen;
- De scriptie afgerond.

Op te leveren (sub)producten

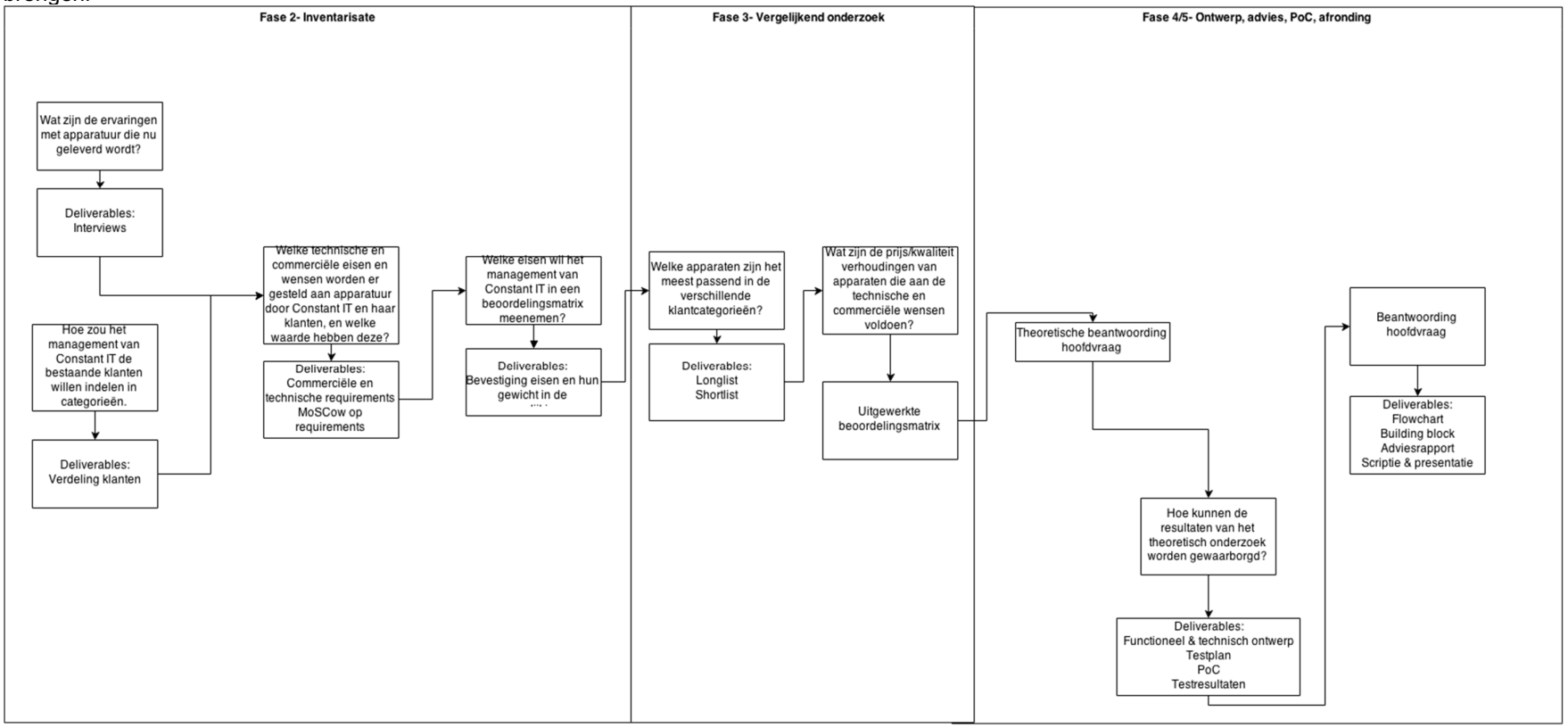
- Documentatie proof of concept met de resultaten;
- Gevulde building blocks
- Adviesrapport;
- Scriptie;
- Presentatie (afstudeerzitting)

Te beantwoorden deelvragen

- Hoe kunnen de resultaten van het theoretisch onderzoek worden getoetst in de praktijk?

9.6 OVERZICHT PROJECTFLOW.

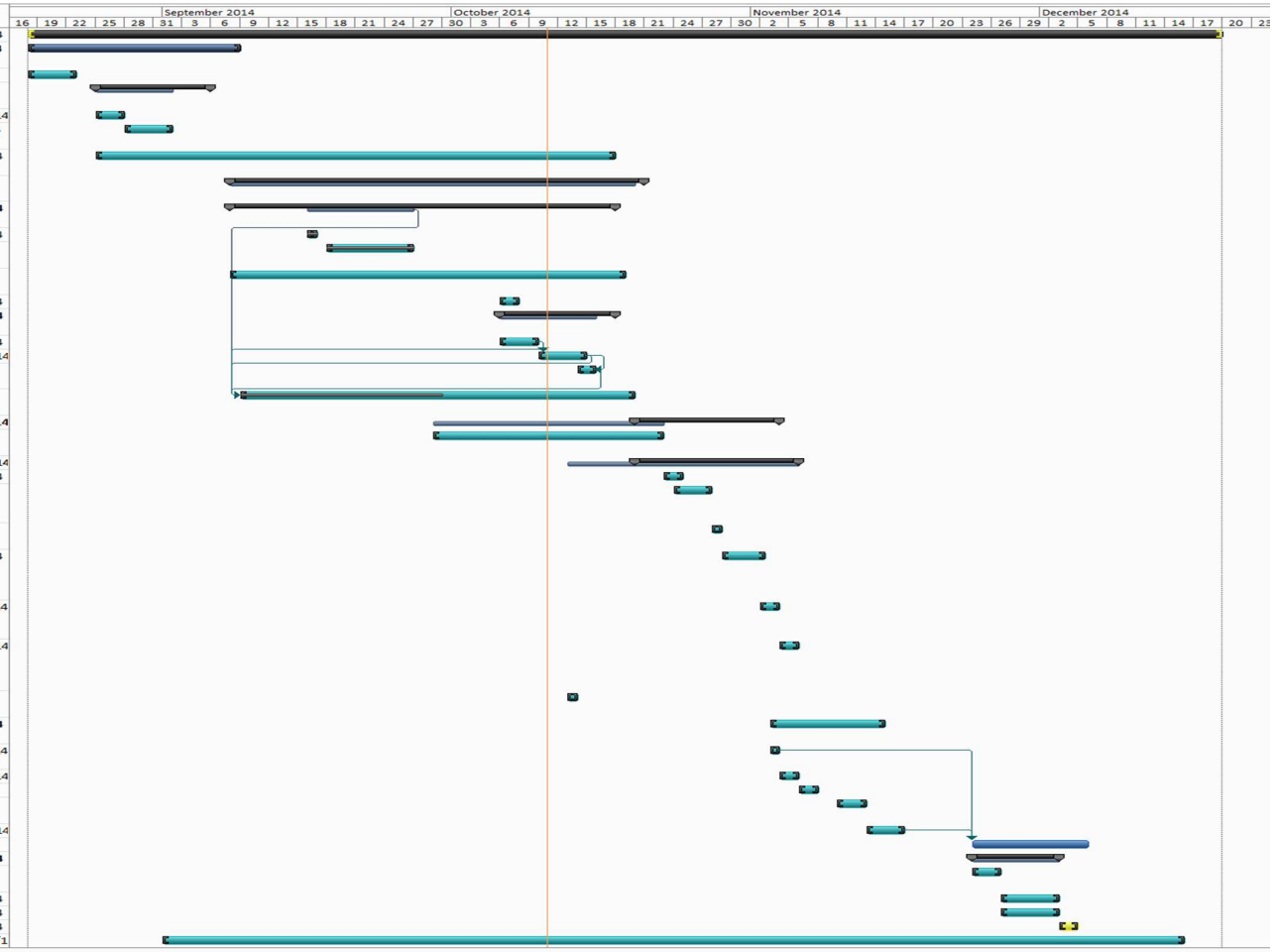
In dit hoofdstuk wordt schematisch weergegeven welke deelvraag welke tussenproducten oplevert. Daarnaast wordt ook inzichtelijk gemaakt welk tussenproduct een “input” vormt voor de volgende deelvraag. Het doel is om met behulp van één overzicht de stroom van het gehele project in kaart te brengen.



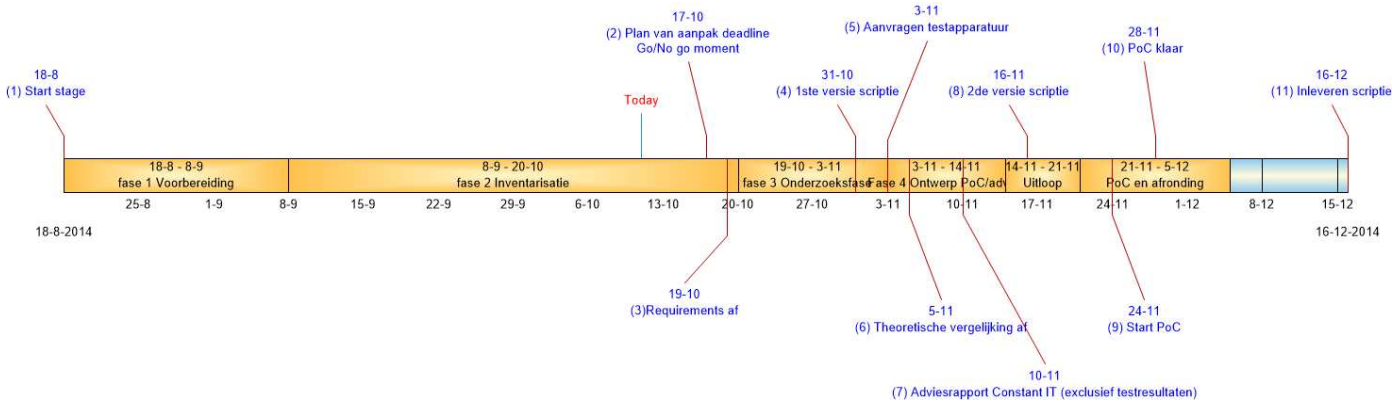
Figuur 17 Projectflow

9.7 PLANNING

ID	Task Mod	Task Name	Duration	Start	Finish
1		Stage / scriptie	90 days	Mon 8/18/14	Fri 12/19/14
2		**Fase 1 Voorbereidings fase**	**16 days**	**Mon 8/18/14**	**Mon 9/8/14**
3		Onderzoek TOGAF	5 days	Mon 8/18/14	Fri 8/22/14
4		**Onderzoek te gebruiken methoden**	**10 days**	**Mon 8/25/14**	**Fri 9/5/14**
5		Informatie doorlezen	3 days	Mon 8/25/14	Wed 8/27/14
6		Gekozen methoden verwerken in PvA	3 days	Thu 8/28/14	Mon 9/1/14
7		Plan van aanpak schrijven / aanpassen	40 days	Mon 8/25/14	Fri 10/17/14
8		**Fase 2 Inventariserende fase**	**31 days**	**Mon 9/8/14**	**Mon 10/20/14**
9	✓	**Eisen en wensen inventariseren**	**30 days**	**Mon 9/8/14**	**Fri 10/17/14**
10	✓	Gesprek Bas en Bila	1 day	Tue 9/16/14	Tue 9/16/14
11	✓	Verwerken resultaten gesprek	7 days	Thu 9/18/14	Fri 9/26/14
12		Deskresearch naar huidige producten	30 days	Mon 9/8/14	Sun 10/19/14
13		Klanten verdelen	2 days	Mon 10/6/14	Tue 10/7/14
14		**Interviews naar ervaringen**	**10 days**	**Mon 10/6/14**	**Fri 10/17/14**
15		Interviews maken	4 days	Mon 10/6/14	Thu 10/9/14
16		Interviews afnemen	3 days	Fri 10/10/14	Tue 10/14/14
17		Interviews verwerken	2 days	Tue 10/14/14	Wed 10/15/14
18		Requirements document maken	30 days	Tue 9/9/14	Sun 10/19/14
19		**Fase 3 Onderzoeksfase**	**11 days**	**Mon 10/20/1**	**Mon 11/3/14**
20		Onderzoek apparaten op de markt	18 days	Mon 9/29/14	Wed 10/22/14
21		**Productonderzoek**	**13 days**	**Mon 10/20/1**	**Wed 11/5/14**
22		Longlist maken	2 days	Thu 10/23/14	Fri 10/24/14
23		Apparaten tegen "basic" requirements afstrepen	2 days	Fri 10/24/14	Mon 10/27/14
24		Shortlist maken (obv producten uit	1 day	Tue 10/28/14	Tue 10/28/14
25		Apparaten tegen "specific" requirements afstrepen.	3.5 days	Wed 10/29/14	Sun 11/2/14
26		Prijs/kwaliteit verhoudingen in kaart brengen	2 days	Sun 11/2/14	Mon 11/3/14
27		Beoordelingsmatrix vullen en uitwerken(levert "beste" producten op	2 days	Tue 11/4/14	Wed 11/5/14
28		Informatie vergaren mbt leenproducten	1 day	Mon 10/13/14	Mon 10/13/14
29		**Fase 4 Ontwerp PoC/ advies**	**10 days**	**Mon 11/3/14**	**Fri 11/14/14**
30		Aanvragen leenapparatuur poc	1 day	Mon 11/3/14	Mon 11/3/14
31		Functioneel ontwerp	2 days	Tue 11/4/14	Wed 11/5/14
32		Technisch ontwerp	2 days	Thu 11/6/14	Fri 11/7/14
33		Adviesrapport schrijven (exclusief	3 days	Mon 11/10/14	Wed 11/12/14
34		Testplan maken	3 days	Thu 11/13/14	Sun 11/16/14
35		**Fase 5 PoC en afronding**	**10 days**	**Mon 11/24/1**	**Fri 12/5/14**
36		**PoC**	**7 days**	**Mon 11/24/1**	**Tue 12/2/14**
37		Omgeving opzetten	3 days	Mon 11/24/14	Wed 11/26/14
38		Tests uitvoeren	4 days	Thu 11/27/14	Tue 12/2/14
39		Bevindingen docume	4 days	Thu 11/27/14	Tue 12/2/14
40		Flowchart maken	2 days	Wed 12/3/14	Thu 12/4/14
41		Scriptie	76 days	Mon 9/1/14	Mon 12/15/1



Figuur 18 Gantt chart



Figuur 19 Milestone planning

Overzicht belangrijke data	
Plan van aanpak	17-10-2014
1ste versie scriptie	31-10-2014
Adviesrapport Constant IT	14-11-2014
2de versie scriptie	16-11-2014
Laatste versie scriptie	16-12-2014

Tabel 28 Overzicht belangrijke data

Taak	Geplande Uren
Voorbereidingsfase	
Onderzoek TOGAF	40
Onderzoek te gebruiken methoden	20
PvA maken	40
Inventariserende fase	
Gesprek requirements met collega's en verwerken informatie	**20**
Interviews maken	16
Interviews afnemen	20
Interviews verwerken	40
MoSCow + beoordelingsmatrix	40
Requirementsdocument maken	40
Onderzoeksfase	
Onderzoek apparaten op de markt	40
Longlist maken en vullen	16
Shortlist maken en vullen	8
Prijs/kwaliteit uitrekenen	16
Beoordelingsmatrix	16
Proof of concept en advies	
Adviesrapport maken	40
Flowchart maken	16
Testplan	24
PoC en afronding	
Proof of concept	100
Tests uitvoeren en documenteren	40
Scriptie	150
Presentatie (afstudeerzitting)	20
Flowchart maken	8
TOTAAL	750

Tabel 29 Urenschatting taken.

10 DE PLAATS IN DE ORGANISATIE

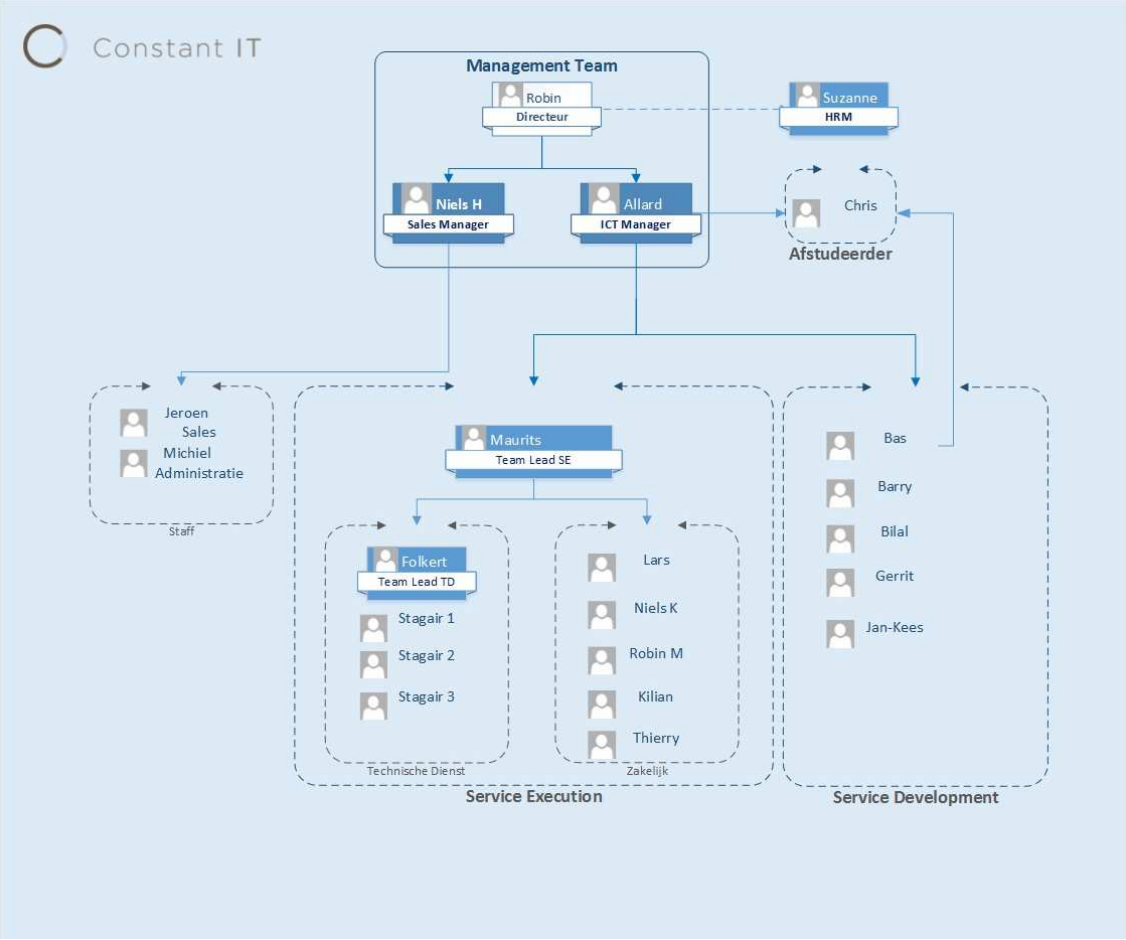
Tijdens de afstudeerperiode zal er meegedraaid worden op de afdeling systeembeheer. Deze afdeling valt onder te verdelen in twee subafdelingen namelijk:

Service Development

Hier wordt gewerkt aan projecten, worden nieuwe services ontwikkelden worden geëscaleerde incidenten opgelost. Projecten omvatten bijvoorbeeld het migreren van servers of het vernieuwen en/of uitbreiden van de netwerkinfrastructuur. Daarnaast functioneren ze ook als een vraagbaak voor de Service Execution afdeling.

Service Execution.

Hier wordt het reactief beheer gedaan. Klanten die problemen ervaren met de dienstverlening van Constant IT kunnen bellen of e-mailen waarna er een ticket aangemaakt wordt in het ticket systeem. Afhankelijk van het SLA dat Constant IT met de klant in kwestie heeft afgesproken krijgt een ticket meer prioriteit.



Figuur 6 Overzicht projectorganisatie

11 RISICO'S

De risico's die we tijdens dit afstudeerproject kunnen verwachten zijn;

Risico ID	Risico	Maatregel	Kans	Impact
1	Uitval afstudeerder, docentbegeleider of één van de begeleiders van Constant IT	Er wordt voor het afstuderen een strakke planning gehanteerd. Bij ziekte zal dit op tijd gemeld moeten worden aan Constant IT en de docentbegeleider. De verloren tijd zal ingehaald moeten worden.	Laag	Hoog
2	De doelen van het project worden niet behaald of er wordt afgeweken van de doelen van Constant IT.	Meermaals per maand een dialoog aan gaan met de eindverantwoordelijke en de docentbegeleider ten behoeve van kwaliteitsbewaking.	Laag	Laag
3	De inventarisatie van de huidige apparaten is niet volledig omdat Constant IT de gegevens niet te verkrijgen zijn.	De inventarisatie van de huidige apparaten wordt achterwege gelaten. Er worden in plaats hiervan interview gehouden om de ervaringen te achterhalen. Daarnaast staan er ook apparaten in Kaseya wat Constant IT gebruikt om apparaten te beheren welke gebruikt kunnen worden om tenminste een beeld te schetsen.	Hoog	Laag
4	Leenapparaten voor het proof of concept zijn niet beschikbaar.	Er moet tijdig met sales contact opgenomen worden om apparaten te regelen voor het proof of concept. Daarnaast zal de afstudeerder zelf ook contacten moeten leggen met de fabrikanten van wie de apparatuur in het proof of concept getest moet worden/	Hoog	Hoog
5	Scriptie is niet van voldoende kwaliteit	De scriptie wordt geëvalueerd op inhoud door de twee begeleiders. Daarnaast zal er een taalkundige controle uitgevoerd worden door een andere collega.	Laag	Hoog

Tabel 30 Risico's

12 DE PROJECTORGANISATIE

12.1 DE OPDRACHTGEVER

Opdrachtgever in dit project is de ICT manager van Constant IT Allard Borgart. Hij zal het project ook overzien en zal feedback geven op de kwaliteit van het werk wanneer nodig.

12.2 DE OPDRACHTNEMER

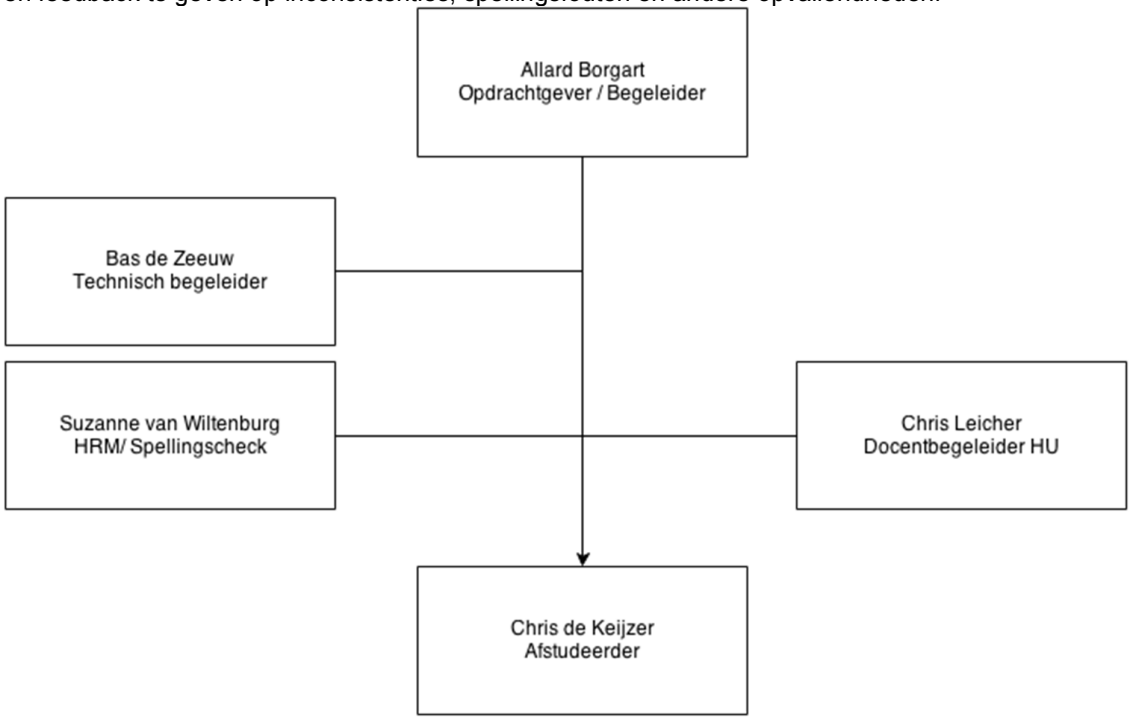
Chris de Keijzer is de opdrachtnemer binnen dit éénmansproject en zal dus alle projectrollen vervullen. Er zal door de opdrachtnemer verantwoordelijkheid gedragen worden voor de oplevering van de correcte eindproducten zoals deze beschreven staan in dit plan van aanpak.

12.3 DOCENTBEGELEIDER

Chris Leicher is aangewezen al docentbegeleider voor dit afstudeerproject. Hij ondersteund en bewaakt de kwaliteit van de opdracht door de afstudeerder te voorzien van feedback. Er zal minimaal eenmaal per week een contact moment zijn via mail of telefonisch gesprek.

12.4 OVERIGE PARTIJEN

Bas de Zeeuw voorziet het afstudeerproject van technische begeleiding, hij is expert op het gebied van netwerken. Daarnaast heeft hij een duidelijk beeld van de doelen van dit afstudeerproject. De afstudeerder zal eenmaal per week naast Bas werken om op deze manier eenvoudig vragen te kunnen stellen met betrekking tot de technische aspecten.
Suzanne van Wiltenburg ondersteund de afstudeerder door de kwaliteit van de scriptie te controleren en feedback te geven op inconsistenties, spellingsfouten en andere opvallendheden.



Figuur 20 Overzicht projectorganisatie

13 DE BEDRIJFS-/PERSOONSGEGEVENS

Naam: Christiaan de Keijzer
E-mail: chris.dekeijzer@student.hu.nl
Telefoonnummer: 06-10181296
Bedrijfsnaam: Constant IT
Website: www.constant.it
Adres: Oosteinde 1
Postcode: 1017 WT, Amsterdam
Telefoonnummer: 020–6121016
Algemene e-mail: info@constant.it
Stagebegeleider:
Naam: Allard Borgart
Functie: ICT Manager
E-mail: a.borgart@constant.it
Personeelsmanager:
Naam: Suzanne van Wiltenburg
Functie: Personeelsmanager
E-mail: s.vanwiltenburg@constant.it
Docentbegeleider:
Naam: Chris Leicher
E-mail: Chris@Leicher.com
Telefoonnummer: 06-18390924

REFERENTIES

Bloomsbury Buisiness Library. (2007). *Bibliotheek HU*. Retrieved from http://eds.b.ebscohost.com.www.dbproxy.hu.nl/eds/detail/detail?vid=9&sid=86c9aa1f-d2e5-472c-ab90-e445aca8918d%40sessionmgr198&hid=101&bdata=Jmxhbmc9bmwmc2l0ZT1lZHMtbGl2ZQ%3d%3d##db=bsh&AN=26741174

International Institute of Buisiness Analysis. (2009). *a guide to the business analysis body of knowledge (babok guide)* . Retrieved from http://www.iowadnr.gov/: http://www.iowadnr.gov/portals/idnr/uploads/Iowa%20Outdoors%20News/2011/BABOK%20Version2.pdf

Investorwords. (n.d.). *Definition of proof of concept*. Retrieved from Investorwords: http://www.investorwords.com/3899/proof_of_concept.html

Open Group (Building Blocks). (2011). *TOGAF Overview*, 9.1. Retrieved from www.opengroup.com: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap37.html

Open Group (Introduction to TOGAF). (2011). *Introduction to TOGAF*. Retrieved from Opengroup.com: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap01.html

Sogeti. (2011). *TMap next*. Retrieved from TMap: http://www.tmap.net/tmap

Steehouder, M. (2012). *Leren Comminuceren* (Vol. 2). Groningen/Houten: Noordhoff Uitgevers B.V.

Utrecht, H. B. (2013). Pakketselectie van de HU. Utrecht.

BIJLAGE

DE OPDRACHT ZOALS OPGELEVERD DOOR CONSTANT IT

Op het gebied van netwerken zouden we graag een aantal 'templates'/standaard oplossingen willen hebben, onder te verdelen in een aantal segmenten. Geen wildgroei meer aan exotische routers/firewalls maar een aantal “proven” oplossingen welke binnen de gestelde budgeten vallen. Voor elk onderdeel/segment zou je dan productvergelijking kunnen toepassen (soort best-buy guide a la tweakers).

- Unmanaged switch;
- Managed switch L2 (QoS, vlan's, snmp);
- Managed switch L3 (QoS, vlan's, snmp, ip routing);
- Basic router/firewall (NAT, SNAT, FW rules);
- Advanced router/firewall (NAT, SNAT, FW rules, Multi-WAN, IPsec, BOVPN, LDAP/AD integratie, QoS).

Het is wenselijk om ook de mogelijkheden tot monitoring in acht te nemen.

CONCEPT INDELING SCRIPTIE

- Voorwoord
- Managementsamenvatting
- Inhoudsopgave
- Verklarende woordenlijst
- Inleiding
- Organisatie
    - Bedrijfsprofiel
    - De positie binnen Constant IT
    - Organigram
- De opdracht
    - Aanleiding
    - Kwestie
    - Doelstelling
    - Opdrachtomschrijving
    - Deelvragen
    - Producten
- Antwoord Deelvraag 1
- Antwoord Deelvraag 2
- Antwoord Deelvraag 3
- Antwoord Deelvraag 4
- Antwoord Deelvraag 5
- Antwoord Deelvraag 6
- Antwoord Deelvraag 7
- Antwoord Deelvraag 8
- Antwoord Deelvraag 9
- Conclusie.
- Aanbevelingen
- Bronvermelding
- Bijlage
    - Interviews
    - Onderzoeksrapport
    - Functioneel ontwerp
    - Technisch ontwerp
    - Testdocumentatie
    - Adviesrapport
    - Flowchart
    - Evaluatie

CONTRACT AFSTUDEEROPDRACHT

Institute for ICT
Nijenoord 1, 3552AS, Utrecht
NB: Dit contract dient te worden opgenomen als vast onderdeel van het plan van aanpak

HOGESCHOOL UTRECHT

Datum 15 – 10 – 2014

Naam student	Chris de Keijzer
Opleiding	System and Network Engineering (Voltijd)
Adres student	Reguliershof 16
Postcode / plaats student	1383AN, Weesp
Studentnummer	1591134
Telefoonnummer privé	0610181290
E-mailadres	chris.dekeijzer@student.hu.nl

Naam bedrijf	Constant IT
Adres bedrijf	Oosteinde 1
Postcode / plaats bedrijf	1017WT, Amsterdam
Naam bedrijfsbegeleider	Allard Borgart
Telefoonnummer bedrijfsbegeleider	0206121016
E-mailadres bedrijfsbegeleider	A.borgart@constant.it

Beoogde datum afstuderen januari 2015

Geheimhouding geaccordeerd door de HU op [i] .....

Ondergetekenden verklaren akkoord te gaan met de inhoud van het aangehecht Plan van Aanpak.

Student .....

Docentbegeleider .....

Bedrijfsbegeleider [ii] .....

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

BIJLAGE 2: EVALUATIE CHRIS DE KEIJZER

EVALUATIE PROCESGANG (FEITELIJK)

Eerste weken & PvA
De eerste weken zijn gebruikt om de organisatie te leren kennen, een beeld te vormen van de opdracht en een start te maken met het PvA. Het maken van het PvA ging in eerste instantie goed, echter moest deze vaker aangepast worden dan verwacht waardoor er veel tijd verloren ging. Het veelvuldig bezig zijn met het PvA heeft wel de opdracht scherp gesteld voor alle partijen.

Requirements
Het verzamelen van requirements is begonnen terwijl het PvA nog niet compleet was, op deze manier kon de opdracht begonnen worden terwijl het PvA werd nagekeken en de tijdsdruk verminderen. De requirements zijn grotendeels afkomstig van de netwerkspecialisten maar er zijn ook veel relevante eisen door de afstudeerder bedacht waardoor uiteindelijk een compleet beeld is ontstaan waar Constant IT ook tevreden mee is. De interviews die gehouden zijn hebben wel resultaten opgeleverd, echter omdat niet iedereen het over dezelfde apparatuur heeft gehad in de beantwoording van de open vragen ontstaat er geen perfect beeld.

Vergelijkend onderzoek
Met behulp van de gekozen methode viel er met wat aanpassingen zeer goed te creëren wat Constant IT zocht en dat was het in een oogopslag zichtbaar maken van de resultaten van het onderzoek. Dit resulteerde in een aantal grote tabellen die behoorlijk effectief waren. Tijdens dit deel van het project zijn er geen grote problemen ondervonden. Het enige probleem was dat er gekozen is voor een systeem met vinkjes waardoor een eis als " VPN functionaliteit", waarbij meestal een maximaal nummer aan tunnels gespecificeerd is erg lastig te kwantificeren wordt. Een vinkje toont immers niet aan of er 2 of 200 VPN tunnels gemaakt konden worden. Omdat Constant IT graag alles in 1 overzicht wilde is er besloten geen losse beoordelingsmatrix te maken.

Testplan & PoC
Uit het onderzoek kwam dat er een Cisco SG300 en een Watchguard XTM26 getest moesten worden, echter was het maximaal haalbare een SG200 en XTM26 omdat fabrikanten niet mee wilden werken. Dit heeft echter niet veel invloed gehad op het testen maar wel op de resultaten hiervan, er is immers een ander apparaat gebruikt. De tests werden bemoeilijkt omdat het testplan nog niet helemaal af was toen het testen al begon, uiteindelijk zijn de tests en het testplan bijna tegelijk gemaakt.
Uiteindelijk zijn de resultaten nog in building block gezet om een goed overzicht te krijgen van de resultaten en de standaardisatie.

Scriptie en aansluiting resultaten op PvA
De scriptie, dat een resultaat is van alle deelvragen is gedurende de stage goed bijgehouden. Zodra deelvragen beantwoord konden worden is dit ook gedaan om tijd te winnen.
De resultaten van het project sluiten goed aan op wat Constant IT wilde, er bestaat nu een kleine selectie apparaten die voldoen aan de eisen. Hiervan is een enkele categorie getest in een PoC wat conform het plan van aanpak is. Als het proces bekeken wordt valt te concluderen dat dit eigenlijk volledig als gepland is verlopen met als aanmerking dat de tijdsinschatting en de daadwerkelijke tijd niet hebben geklopt. De building blocks geven weer wat er geleverd is en welke basis configuratie dit heeft.

PERSOONLIJKE EVALUATIE (RETROSPECTIEF)

Eerste weken & PvA
Zoals gezegd heb ik in de eerste weken de organisatie leren kennen, dit hield in dat ik meewerkte met de directe collega's wat ik een goede manier vond om met de interne systemen bekend te raken. In de tussentijd ben ik begonnen met het PvA, ik vond het fijn dat ik erg snel wist hoe ik dit project wilde aanpakken maar het op papier zetten bleek iets lastiger dan verwacht. Het PvA kwam vaak terug voor feedback waardoor ik er uiteindelijk helemaal gek van werd, echter heeft al deze feedback er wel voor gezorgd dat het PvA van goede kwaliteit is. Dit is ook het eerste project waar het PvA echt relevant is, in de themaopdrachten op school wordt hier niet voldoende mee gedaan. Het hele proces van het maken van het PvA was voor mij een groot leermoment.

Requirements

Het verzamelen / bedenken van de requirements verliep soepel en ik ben tevreden met de keuze van het maken van tabellen waarin de requirements staan. Er zijn in totaal behoorlijk wat categorieën en eisen maar de tabellen helpen naar mijn mening om het geheel nog enigszins overzichtelijk te houden. Ik ben minder tevreden over de interviews die gehouden zijn, dit had niet te maken met de inzet van de betrokken partijen maar wel met de tijd. Tegen de tijd dat de interviews gehouden konden worden stond er al aardig wat druk op de ketel, ik moest immers gaan beginnen met het vergelijken. De interview vragen zijn dus overhaast gemaakt en zorgen ervoor dat er niet altijd een scherp antwoord mogelijk is, ik heb dit tijdens de interviews mondeling wat scherper proberen te maken door voorbeelden te geven en uitleg te geven. Uiteindelijk ben ik blij dat er toch nog resultaten uit de interviews gekomen zijn.

Vergelijkend onderzoek

Toen alle requirements in kaart waren gebracht was het tijd om onderzoek te doen, het eerste waar ik tegen aan liep was dat ik niet wist welke merken allemaal in de vergelijking moesten komen. Omdat ik in het PvA niets hierover gezegd heb had eigenlijk alles hierin gekund, uiteindelijk heb ik mijzelf gelimiteerd tot de grotere en bekendere merken. Na het longlisten waar ik wel wat moeite had om het aantal apparaten terug te dringen omdat veel apparaten aardig gelijk zijn kon ik starten met het shortlisten en de beoordelingsmatrix. Ik heb eerst alles op de shortlist gezet waarna bleek dat de daaruit volgende beoordelingsmatrix veel te groot werd. Persoonlijk vind ik het een goede keuze dat ervoor gekozen is om de shortlist en de beoordelingsmatrix in één tabel te doen. Door de shortlist en de beoordelingsmatrix in een enkele tabel te doen is het eindresultaat per categorie te zien in één oogopslag en dat is wat Constant IT graag wilde.

Testplan & PoC

Bij het PoC verliep het aanvragen van de testapparatuur goed, ik was al gewaarschuwd dat het enige tijd kon duren dus hier was ik op tijd mee begonnen. Wat mij erg tegenviel was dat de verschillende fabrikanten en leveranciers niet mee wilden werken met het verlenen van testapparatuur. Ik begrijp het wel, want het is apparatuur die daarna eigenlijk niet meer te verkopen is maar je hoort vaak dat mensen testapparatuur kunnen verkrijgen. Uiteindelijk was ik erg blij dat er toch apparatuur gekomen is waarmee te testen viel, dit was apparatuur die uiteindelijk naar een klant moest en bestond uit een Watchguard XTM26 en een Cisco SG200.
De procesgang van het PoC staat beschreven is het testplan. Ik denk dat ik iets te laat begonnen ben met het testplan waardoor ik uiteindelijk in de nacht moest werken. Doordat er maar bepekte tijd was om te testen (de apparatuur moest namelijk naar de klant) is de kwaliteit van het testplan niet perfect maar zeker werkbaar en door het toevoegen van een casus is er ook veel meer technische diepgang behaald. De resultaten zijn naar mijn mening duidelijk en zeker bruikbaar in de scriptie.

Als laatst zijn er building blocks gemaakt op basis van TOGAF. Hier kwam ik echt pas veel te laat aan toe en was een beetje een haastklus. Echter denk ik wel dat de building blocks gebrukt gaan worden hoewel dit misschien niet in de huidige vorm is.

Concluderend is het naar mijn mening zo dat de opdracht enorm breed was, breder dan dat ik aanvankelijk dacht omdat er verschillende categorieën waren waarmee een productvergelijking gemaakt moest worden. Als er minder categorieën waren geweest had ik meer gedetailleerd kunnen vergelijken, maar dan waren de door Constant IT beoogde resultaten niet behaald.

De tijd die ik bij Constant IT gehad heb gaat wat mij betreft de boeken in als succesvolle en vooral leuke tijd. Tijdens het afstuderen ben ik goed begeleid door zowel Allard als Bas vanuit Constant IT. Naast het afstuderen vond ik het ook erg leuk om op training te gaan bij Watchguard om daar de basis te leren, er zijn niet veel stagebedrijven die zo'n kans geven. Uiteindelijk mocht ik de geleerde kennis in praktijk brengen door voor een klant een Watchguard en twee switches in te stellen. Daarnaast vind ik het prettig dat Constant IT ook tevreden is met de geleverde resultaten en documentatie.
Ook mijn ervaringen met Chris Leicher zijn goed, in het begin werd ik wel een beetje gek van de hoeveelheid aanpassingen op het PvA maar uiteindelijk heb ik ook ingezien dat dit tot een goed resultaat heeft geleid. Daarnaast geeft Chris altijd goede feedback maar hij houdt je niet aan het handje. Als je het echt even niet meer weet is Chris er om begeleiding te geven, dit vond ik zelf zeer prettig.

Requirements

Constant IT

26 augustus 2014, Chris de Keijzer
Opleiding: System & Network engineering
Studentnummer: 1591134
Telefoonnummer: 06-10181296
Versie: 1.0

1 DOCUMENTINFORMATIE

Documentbeheer en Goedkeuring

Versie	Auteur	Opmerkingen	Document Eigenaar	Datum
0.11	Chris de Keijzer	Eerste draft	Chris de Keijzer	13-10-2014
0.2	Chris de Keijzer	Eerste versie, feedback verwerkt	Chris de Keijzer	28-10-2014
0.3	Chris de Keijzer	Versie 1, feedback verwerkt	Chris de Keijzer	31-10-2014
1.0	Chris de Keijzer	Final, laatste feedback verwerkt	Chris de Keijzer	5-11-2014

Dit document is beoordeeld door

Versie	Naam	Functie	Datum beoordeling
0.11	Allard Borgart	ICT manager	22-10-2014
0.2	Allard Borgart	ICT manager	27-10-2014
0.2	Bas de Zeeuw	Technical specialist	27-10-2014
0.3	Allard Borgart	ICT manager	4-11-2014
0.3	Bas de Zeeuw	Technical specialist	4-11-2014

Dit document is goedgekeurd door

Versie	Naam	Functie	Datum beoordeling
1.0	Allard Borgart	ICT manager	5-11-2014

INHOUDSOPGAVE

Inhoudsopgave 3
Verklarende woordenlijst 4
1 Inleiding 5
2 Verdeling klanten 5
3 Eisen en wensen Constant IT 7
3.1 Globale eisen 7
3.2 Specifieke eisen 9
3.2.1 Switches 10
3.2.2 Toekomstvastheid 10
3.2.3 Beheerbaarheid 12
3.2.4 Features 14
3.2.5 Veiligheid 15
3.2.6 Ondersteuning & fabrikant 17
3.3.1 Router/firewalls 18
3.3.2 Toekomstvastheid 18
3.3.3 Beheerbaarheid /betrouwbaarheid 20
3.3.4 Features 22
3.3.5 Veiligheid 25
3.3.6 Ondersteuning & fabrikant 27
4 Ervaringen 28
4.1 Uitwerking interviews in nummers 29
Figurenlijst 31
Bronvermeldingen 32
Bijlage 1 Interview Service Development & Service Execution 33
Service development 33
Service execution 38
Bijlage 2 VPN bandwidth reports 43
FW-LM-Metsu 43
FW-LM-Rustenburg 47
FW-AVC-DC 51

VERKLARENDE WOORDENLIJST

Apparaat	Geleverde hardware, dit is een switch, router of firewall.
LAN	Local Area Network, ofwel een intern netwerk
Layer 2	Layer 2 apparatuur zorgt ervoor dat er signalen over de netwerkkabels gaan zonder. Doorsturen gebeurd op basis van het MAC adres.
Layer 3	Layer 3 apparatuur werkt op basis van IP adressen, Met behulp van routing protocollen kunnen andere netwerken gevonden worden.
Longlist	Een lijst met producten die voldoen aan de globale requirements.
Prijs kwaliteitverhouding	Een waarde toekenning van een product gedeeld door de prijs
Shortlist	Een lijst met apparaten die aan eisen en wensen voldoen en waar eventueel goede ervaringen mee zijn. Deze voorkeurslijst is gebaseerd op de longlist
Sizing	Deze term houdt in dat apparatuur passend moet zijn bij een klantcategorie.
VPN	Een Virtual Private Network is een verbinding die via het internet (WAN) naar een andere locatie loopt waarmee het lijkt alsof er in het LAN gewerkt wordt. Deze verbindingen zijn veelal versleuteld.
WAN	Met een Wide Area Network wordt het internet bedoeld.

1 INLEIDING

Dit document bevat de requirements waaraan de apparaten die aan bod komen in het afstudeerproject moeten voldoen om in aanmerking te komen voor de standaardisatie. Er zal in dit document ook informatie gegeven worden met betrekking tot de onderverdeling van klanten. Hoofdstuk twee bevat de verdeling van de klanten alsmede de argumentatie daarvoor. In hoofdstuk drie worden de eisen en wensen van Constant IT beschreven met de onderverdeling in het achterhoofd. In hoofdstuk vier worden de resultaten van de interviews met de medewerkers van Constant IT beschreven ten behoeve van het achterhalen van de ervaringen.

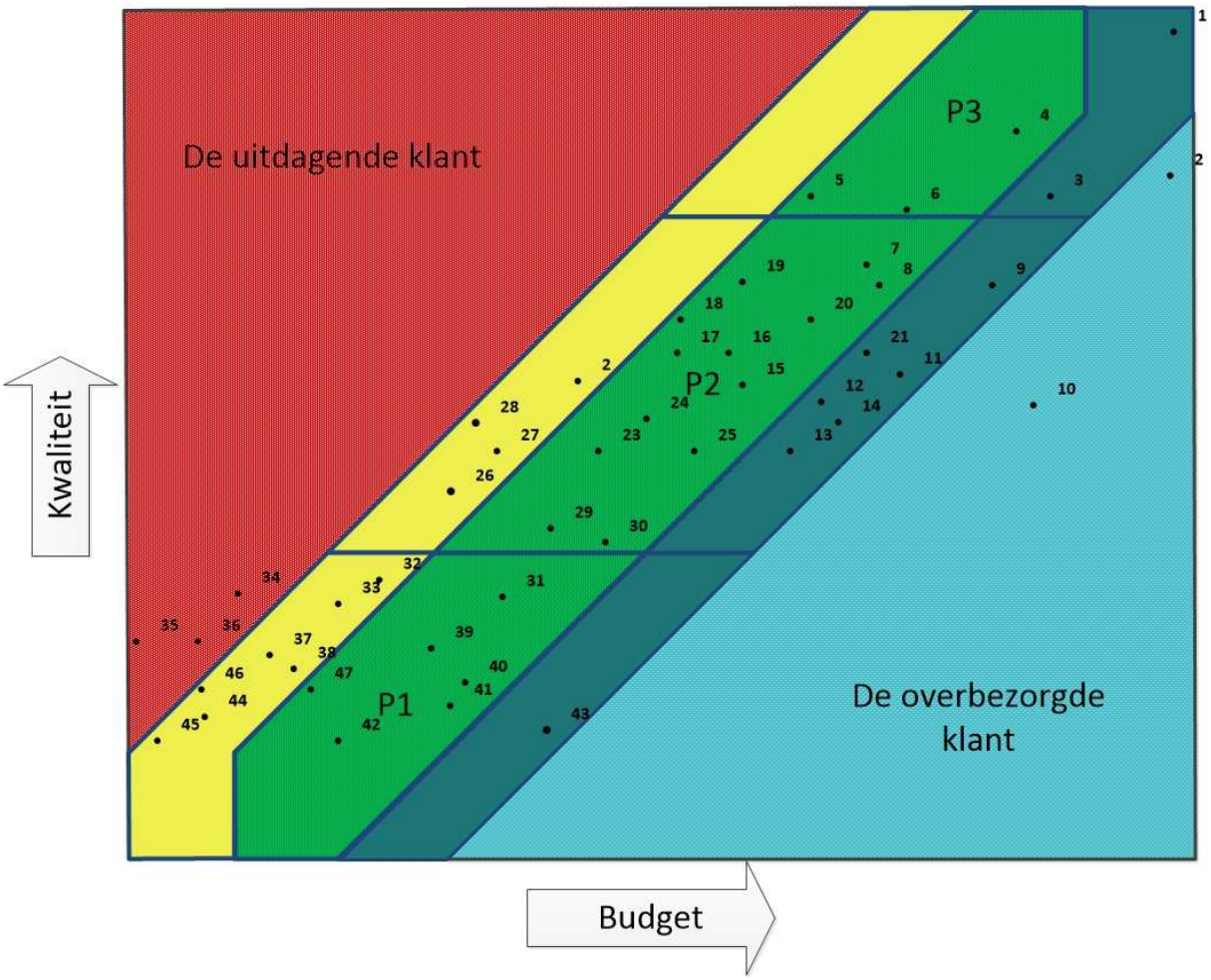
2 VERDELING KLANTEN

Constant IT heeft een groot aantal klanten die elk sterk van elkaar verschillen. Omdat Constant IT wil standaardiseren zullen ook de klanten in categorieën verdeeld moeten worden.
Aan de hand van gesprekken met ICT manager/ stagebegeleider Allard Borgart en directeur Robin Kuipers zijn de klanten die een SLA hebben onderverdeeld in categorieën en in een model verwerkt. Het model is verdeeld op basis van budget en het niveau van kwaliteit dat verwacht wordt. Voor de vergelijking wordt de realistische klant gebruikt, deze lijn die met groen is aangegeven gaat ervan uit dat een klant wil betalen voor wat hij nodig heeft. Er zijn uiteraard ook uitzonderingen, deze worden aangegeven in de hoeken met de onrealistische en de overbezorgde klantgroep. Hoe verder een klant richting de uitdagende hoek zit hoe meer overtuiging deze klant nodig heeft om hem te laten investeren. Een overbezorgde klant is het compleet tegenovergesteld, deze klant denkt dat duurder beter is terwijl de technische eisen dit niet verantwoorden waardoor deze klant geadviseerd dient te worden.
De groene lijn die de realistische klant weergeeft is verdeeld in drie categorieën, deze categorieën zijn de basis van de productvergelijking.

P1: “Klein zakelijk”
Dit zijn de kleinste klanten, zowel budgettair gezien als qua eisen. Deze klanten zoeken voor een goede prijs eenvoudige apparatuur die kan voorzien in basisconnectiviteit.

P2 “MKB”
Deze categorie vormt het grootste deel van de klanten van Constant IT, het midden en klein bedrijf. Deze klanten houden zich druk bezig met de continuïteit van de bedrijfsvoering waardoor er vanuit IT oogpunt complexere eisen en wensen ontstaan.

P3 “MKB+”
Dit zijn de grootste klanten van Constant IT, qua IT zitten zij net iets onder enterprise niveau qua IT apparatuur. De eisen verschillen niet veel met die van de P2 categorie maar er wordt wel meer waarde gehecht aan het beheren van de verschillende werknemers door toegang te controleren. Daarnaast doordat er meer werkplekken zijn die aangestuurd moeten worden zal er zwaardere apparatuur moeten worden aangeschaft.



Figuur 21 Verdeling klanten Constant IT

3 EISEN EN WENSEN CONSTANT IT.

Dit hoofdstuk beschrijft de eisen en wensen waarvan Constant IT wil dat die in de vergelijking meegenomen worden. De eisen en wensen zijn zeer uiteenlopend en niet alleen gericht op Constant IT zelf maar ook op de klanten. De specifieke eisen zijn tot stand gekomen na aanleiding van gesprekken met de netwerkspecialisten van Constant IT. De globale eisen zijn tot stand gekomen na gesprekken met ICT manager Allard Borgart.

3.1 GLOBALE EISEN

Om tot een longlist te kunnen komen zijn er een aantal basiseisen gedefinieerd in samenwerking met Constant IT die over alle categorieën van toepassing zijn, dit zijn:

- **Prijs**
  Apparaten moeten binnen de budgeten van de klanten vallen. De budgeten zijn weergegeven in de volgende tabellen en verdeeld op switches (L2/L3) en routers en firewalls.

Categorie	Inkooprijs in €
P1	Tot 150
P2	Tot 500
P3	Vanaf 500

Figuur 23 Prijsindeling switches

Categorie	Inkooprijs in €
P1	Tot 200
P2	Tot 700
P3	Vanaf 700

Figuur 22 Prijsindeling routers/firewalls

- **Leverbaarheid**
  Deze eis houdt in dat apparaten te verkrijgen moeten zijn bij de “preferred” leveranciers van Constant IT. Er wordt in dit onderzoek gesteld dat een apparaat op de longlist komt wanneer de levertijd 7 dagen of minder bedraagt.

- **Sizing**
  Sizing betekend dat apparatuur gelimiteerd is tot de grootte van de klanten van Constant IT. (maximaal 100 werkplekken). Voor switches betekend dit dat er een minimaal aantal aansluitingen overwogen wordt, zie ook figuur 5. Voor routers en firewalls is dit iets lastiger in te schatten, daarom is er in overleg gekozen om deze apparaten te schalen op de informatie die op de productpagina’s staat met betrekking tot hoeveelheid aanbevolen gebruikers voor een apparaat. Deze verdeling is in figuur 4 weergegeven.

Categorie	Switchpoorten
P1	Vanaf 16
P2	Tussen 24-48
P3	48+

Figuur 25 Switchpoorten

Categorie	Gebruikers
P1	Tot 15
P2	Tot 50
P3	Tot 100

Figuur 24 Indeling hoeveelheid gebruikers

Naast de eisen die over alle categorieën geldig zijn er ook globale eisen die op bepaalde categorieën van toepassing zijn. Deze staan hieronder gedefinieerd.

Routers / firewalls P1

- **Als goed beoordeeld door externe partij**
  De instap routers lijken vaak sterk op elkaar qua features, echter zijn er wel verschillen in de interface, stabiliteit of algehele bouwkwaliteit. Omdat er eerst nog een longlist gemaakt moet worden is er besloten met Constant IT om eerst reviews van derde partijen te bekijken. Apparaten die door derden als goed of zeer goed worden ervaren zijn de norm.
- **Vlan tagging**
  De switches hebben als must have eis dat er VLAN’s gemaakt moeten kunnen worden, hierdoor is het uitermate wenselijk dat routers VLAN verkeer kunnen onderscheiden.

Routers/firewalls P2 en P3

- **All-in one oplossing**
  Constant IT heeft geen klanten waar het te verantwoorden valt om een losse high end router en firewall te hebben, daarom wordt er gericht op all-in one firewall oplossingen zoals bijvoorbeeld Watchguard en Fortigate welke ook kunnen routeren.

Switches

- **PoE versie beschikbaar**
  Constant IT heeft aangegeven dat er een paar klanten zijn die gebruik maken van PoE. voor deze klanten moet vanuit de standaardisatie ook een oplossing zijn. Daarom is een eis gesteld dat er van switches ook een PoE versie beschikbaar moet zijn.
- **Bereikbaarheid web interface**
  Switches in de P2 en P3 categorieën moeten geconfigureerd kunnen worden via een webinterface. Niet alle medewerkers zijn even ervaren met command line interfaces waardoor een grafische user interface uitermate wenselijk is voor basis werkzaamheden.

Switches P3

- **Stacking functionaliteit**
  Voor de grootste klanten is het noodzakelijk dat de mogelijkheid tot stacking bestaat. Veel fabrikanten springen erg los om met de term stacking, zo zijn er fabrikanten die onder stacking slechts het configureren van meerdere apparaten op één IP adres verstaan. Wat Constant IT echter wil is echte stacking, waarbij er een kabel op 2 switches aangesloten zit die datacommunicatie tussen de switches afhandelt. Op deze manier worden de 2 switches functioneel gezien één switch.

Figuur 26 Voorbeeld stackable switch

3.2 SPECIFIEKE EISEN

De eisen en wensen zijn onderverdeeld in een aantal begrippen die de functionaliteit categoriseren. Deze begrippen zijn, toekomstvastheid, beheerbaarheid, features, veiligheid en ondersteuning.
In het vorige hoofdstuk zijn de klanten verdeeld waarin ook een verdeling tussen de verwachtingen die de klanten hebben van de dienstverlening kenbaar werd gemaakt. Er zijn klanten met hoge eisen aan de dienstverlening en klanten met lagere eisen. In de tabellen die in de hoofdstukken hieronder aan bod komen wordt ook gekeken of een eis wel van toepassing is op een bepaalde klantcategorie. Daarnaast zijn de eisen volgens de MoSCoW methode verdeeld, dit zal later in de vergelijking een rol spelen.

Toekomstvastheid
Toekomstvastheid geeft aan hoe lang een bepaald apparaat mee gaat en compatibel blijft met de nieuwste technologieën. Constant IT wil graag apparatuur aan klanten leveren waar lange tijd mee gedaan kan worden. Onder toekomstvastheid vallen zaken als snelheid en uitbreidbaarheid.

Beheerbaarheid
Hieronder vallen de eisen die te maken hebben met het beheer van apparatuur. Het is voor Constant IT belangrijk dat beheer eenvoudig kan verlopen. Door eenvoudig en dus efficiënt te kunnen beheren worden doorlooptijden van incidenten verkort. Zaken als remote toegang, back-ups en het verkrijgen van notificaties met behoeve tot up-time vallen onder beheerbaarheid.

Features
Onder features vallen de technische zaken die een apparaat moet kunnen en hebben een directe invloed op de snelheid, betrouwbaarheid of beveiliging van een bedrijf. Hoe meer features een apparaat bezig hoe flexibeler het in te zetten valt.

Veiligheid
Onder veiligheid valt alles wat er voor zorgt om indringers en gevaren buiten te houden maar ook om werknemers te limiteren in wat ze kunnen configureren op een apparaat.

Ondersteuning & fabrikant
De keuze van de fabrikant heeft gevolgen voor het verloop van het beheer, de garantieregelingen en ondersteuning op producten. Het is voor Constant IT niet wenselijk om de hoogste lijn van support te zijn omdat de kennis mogelijk tekort kan schieten bij complexe issues. Er wordt gezocht naar een fabrikant die ondersteuning kan bieden wanneer het echt nodig is.

3.2.1 SWITCHES

Dit hoofdstuk beschrijft de eisen en wensen van switches op zowel layer 2 als layer 3. De eisen en wensen zullen onder de tabellen uitgeschreven worden zodat er geen verwarring kan ontstaan of de inhoud. Er is in overleg met Constant IT besloten om switches van layer 2 en layer 3 samen te voegen in één productcategorie omdat de layer waarop de switch werkt afhangt van de gestelde requirements.

3.2.2 Toekomstvastheid

Niveau eisen	Toekomstvastheid	P1 (laag)	P2 (middel)	P3(hoog)
Must have	• Ipv6	V	V	V
	• Alle poorten minimaal 1Gb	V	V	V
	• Stacking P3*	X	X	V
Should have	• Uitbreidbaarheid (extra poorten)	X	X	V
	• Stackable voor grote klanten	X	X	V
	• Mogelijkheden tot failover	X	V	V
Could have	• Support voor 10GE via koper of fiber	X	X	V
	• Stacking**	X	V	X
Won't have				

Figuur 27 Eisen toekomstvastheid switches

*voor P3 switches is stacking een globale functionaliteit die vereist is, echter wordt deze nog eens meegenomen om resultaten in één oogopslag zichtbaar te maken.
** Stacking kan ook relevant zijn voor de P2 categorie, maar dan wel als "could have"

- **IPv6**
  Nieuwe apparatuur kan niet meer zonder IPv6 ondersteuning vanwege het op raken van de IPv4 adressen. Het is aannemelijk dat alle nieuwe hardware deze ondersteuning al ingebouwd heeft echter wordt de eis voor de zekerheid meegenomen.
  (Schellevis, 2012)

- **Alle poorten minimaal 1Gb**
  Tegenwoordig worden er nog wel eens 100Mbit switches geleverd bij klanten, echter zijn 1 Gbit switches nu wel de standaard.
  Constant IT wil exclusief 1 Gbit switches gaan leveren zodat deze door de hoge snelheid een lange tijd mee kunnen.

- **Uitbreidbaarheid (extra poorten)**
  Constant IT heeft klanten die snel groeien waardoor het ideaal zou zijn om switches te leveren die beschikken over ingangen om extra poorten toe te voegen. Op deze manier zou een klant een switch met een klein aantal poorten kunnen kopen en dan wanneer het noodzakelijk is deze switch uitbreiden met extra slots. Een andere mogelijkheid is uitbreiden met SFP

Figuur 28 SFP+ 10 GE expansion van HP [4]

- **Mogelijkheden tot failover**
  Switches worden op veel locaties in de IT infrastructuur ingezet maar vooral bij de “backbone” is het noodzakelijk de mogelijkheid te hebben om switches redundant uit te voeren. Constant IT wil graag dat switches een vorm van failover hebben. Op welke wijze de failover tot stand komt maakt niet uit.

- **Support voor 10GE via koper of fiber**
  Het kan in bepaalde situaties handig zijn om een uplink poort te hebben met een extreem hoge doorvoersnelheid. Deze poorten kunnen ingezet worden voor het stacken van switches of voor het geven van toegang tot snelle netwerkopslag systemen.

- **Stacking**
  Zoals in de globale eisen beschreven is stacking het laten samenwerken van switches zodat deze als één enkel apparaat gezien worden door het netwerk. Deze eis is voor P3 switches al een vereiste om op de shortlist te komen maar ook relevant voor switches in de P2 categorie.

[4] http://img.ncix.com/images/98080_l.jpg

3.2.3 BEHEERBAARHEID

Beheerbaarheid		P1 (laag)	P2 (middel)	P3(hoog)
Must have	• Loggen via webinterface, syslog of mail.	V	V	V
	• Backup en export van configs	V	V	V
	• Remote access via telnet, ssh, web, tool.	V	V	V
Should have	• Notificaties (send mail when down)	X	V	V
	• Console port	X	V	V
	• Reporting op basis van vooraf ingestelde paramaters	X	V	V
	• Diagnostische tools	X	V	V
Could have	• Opties voor centraal beheer	X	V	V
Won't have	• Kaseya integratie	N.V.T	N.V.T	N.V.T

Figuur 29 Eisen beheerbaarheid switches

- **Loggen via webinterface, syslog of mail.**
  Het is noodzakelijk dat Constant IT weet wat er speelt op de apparatuur van klanten waardoor er behoefte is naar een vorm van logging. Het apparaat kan het zelf bijhouden en inzichtelijk maken of Constant IT zelf een server of pakket aanschaffen dat in deze wens voorziet. Belangrijk is dat men iets met de data kan ten behoeve van troubleshooting. Er moet een mogelijkheid zijn om debug levels in te stellen zodat er niet teveel data binnen komt om te verwerken voor Constant IT

- **Backup en export/import van configuraties**
  Bij troubleshooting kan het voor komen dat er een configuratie geback-upt, geëxporteerd of geïmporteerd moeten worden. Het bespaart veel tijd wanneer hier opties voor zijn.

- **Remote access via telnet, SSH(Secure Shell), webpagina, gespecialiseerde tool**
  Het is voor Constant IT noodzakelijk dat er altijd toegang tot een apparaat te krijgen valt omdat er voornamelijk remote support geleverd wordt.
  Onder de verschillende methoden van remote access maken we onderscheid tussen CLI (Command Line Interface) en GUI (Graphic User Interface) based remote access tools:
  Onder de verbindingsmogelijkheden die op CLI basis werken bestaan:
  CLI: TELNET
  SSH
  Onder de verbindingsmogelijkheden die via GUI werken bestaan:
  GUI: WEBCLIENT zonder plug-ins en/of 3rd party apps.
  WEBCLIENT Met plug-ins en/of 3rd party apps zoals Java of Flash
  Applicatie (voorbeeld: Watchguard System Manager, Cisco Network Assistant)
  De voorkeur gaat uit naar SSH, een webclient zonder benodigdheden of een dedicated applicatie.

- **Reporting op basis van vooraf ingestelde paramaters**
  Constant IT wil graag op basis van vooraf gedefinieerde parameters zaken kunnen loggen ten behoeve van reporting. Dit betreft dus het verzamelen van data voor een management summary en technische audit. Hetgeen dat minimaal te zien moet zijn is:

    - WAN bandbreedte
    - VPN bandbreedte

  Voor bovengenoemde aspecten geldt dat in ieder geval de volgende zaken meetbaar zijn of zijn in te stellen:
    - Throughput van de interface (MB)
    - Transfer amount van de interface (Mbps)
    - Mogelijkheid tot aanpassen tijdspanne van de verzamelde informatie (werkuren, dag, week en maand)
    - Overzicht grootgebruikers
        - client transfer amount
        - destination transfer amount

- **Diagnostische tools**
  Voor apparaten is het zeer wenselijk dat er “tools” aan boord zijn waarmee troubleshooting uitgevoerd kan worden. Voor switches zou dit betekenen dat er de mogelijkheid is om te pingen op layer 3 of om te kunnen zien op layer 2 switches dat er stroom over de netwerkverbinding.

- **Notificaties (send mail when down)**
  Op een switch kunnen soms bepaalde poorten belangrijker zijn dan andere omdat daar bijvoorbeeld een server achter hangt. Voor proactief beheer is het wenselijk dat er een mail gestuurd wordt wanneer een poort “down” gaat.

- **Console port**
  Voor Constant IT is het wenselijk om de mogelijkheid te hebben om ook via een console port bewerkingen uit te voeren op een switch in het geval van nood.

- **Opties voor centraal beheer**
  Om het beheer te vereenvoudigen zou Constant IT graag willen dat apparaten opties hebben om naar een server te verbinden voor het beheer. Mogelijke opties zijn:
    - Management suite waarmee meerdere apparaten van hetzelfde merk beheerd kunnen worden in één centrale locatie
    - Deployment suite waarmee installaties naar apparaten kunnen worden verstuurd.

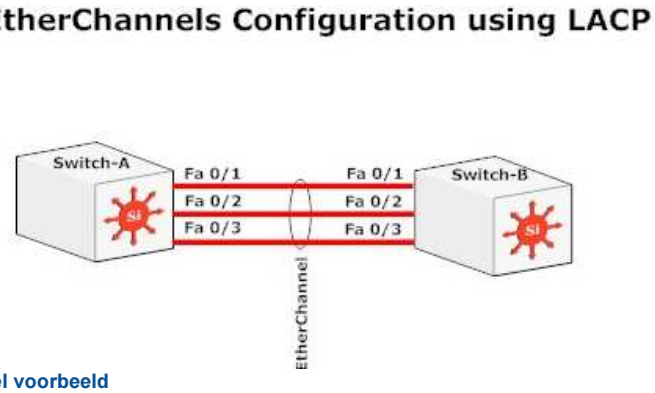
- **Kaseya integratie**
  Een eerder afstudeer stagiair heeft onderzoek gedaan naar de mogelijkheid om Kaseya informatie te laten opvangen van netwerkapparatuur. Destijds bleek dit onmogelijk. Omdat de functionaliteiten niet aanwezig zijn vanuit Kaseya hoeft er in deze vergelijking geen rekening gehouden te worden met integratie.

3.2.4 Features

	Features	P1 (laag)	P2 (middel)	P3(hoog)
Must have	• Etherchannel(LACP)	X	V	V
	• QoS	V	V	V
	• LLDP	X	V	V
	• SNMP	V	V	V
Should have	• Layer 3 functionaliteiten	X	V	V
Could have	• Power over ethernet (PoE)	V	V	V
Won't have				

Figuur 30 Eisen features switches

- **Etherchannel**
  Een etherchannel wordt gevormd wanneer er twee of meer interfaces op een switch in een team gezet worden om op deze manier een theoretische verveelvoudiging van de bandbreedte te behalen. Etherchannels kunnen naast de eerste snelheid ook voorzien in failover zodat verbindingen bijna nooit onderbroken worden. Het protocol dat hier voor gebruikt wordt is het "Link Aggregation Control Protocol" (LACP). Constant IT gebruikt dit bij sommige klanten in de backbone van hun infrastructuur.



Figuur 31 Etherchannel voorbeeld

- **Quality of Service (QoS)**
  Quality of Service zorgt er voor dat bepaalde diensten binnen een netwerk gegarandeerd worden door middel van prioritering. Er zou bijvoorbeeld gekozen kunnen worden om VoIP verkeer hogere prioriteit te geven waardoor er geen pakketten wegvallen en de service altijd stabiel blijft draaien. (Cisco, 2005)

- **Link Layer Discovery Protocol (LLDP)**
  Dit multi-vendor protocol wordt gebruikt om devices zoals IP telefoons automatisch te configureren wanneer deze op een switch worden aangesloten.
  (Rajesh, 2012) (Paul Congdon, 02)

- **Simple Network Management Protocol (SNMP)**
  SNMP is een protocol dat helpt bij het beheer van vrijwel alle apparaten van netwerkapparatuur tot aan servers. SNMP is al jaren een standaard op het gebied van management en Constant IT wil dat alle aangekochte apparaten dit protocol ondersteunen.

Tevens kan er op een later moment gepoogd worden om devices met het interne gebruikte systeem (Kaseya) te koppelen om devices te monitoren en managen.[5]

- **Layer 3 functionaliteiten**
  Layer 3 functionaliteiten in een switch zijn wenselijk omdat er dan gebruikt gemaakt kan worden van IP adressen en routing protocollen. Daarnaast kunnen er ook QoS beslissingen gemaakt worden op basis van IP.

- **Power over ethernet (PoE)**
  Constant IT ziet steeds vaker dat er over gegaan wordt naar IP telefoons die vaak via PoE aangestuurd dienen te worden. Hierdoor is het wenselijk om ook apparaten te kunnen leveren die via PoE stroom kunnen leveren. Er wordt een onderscheid gemaakt tussen de POE en PoE+ standaarden. PoE switches kunnen per poort tot 15.4 watt leveren aan aangesloten apparaten terwijl PoE+ tot wel 25.5 watt kan.

3.2.5 VEILIGHEID

	Veiligheid	P1 (laag)	P2 (middel)	P3(hoog)
Must have	• VLAN	V	V	V
Should have	• VTP	X	X	V
	• Security levels instellen	X	V	V
	• ACL	X	X	V
Could have				
Won't have				

Figuur 32 Eisen veiligheid switches

- **VLAN (Virtual Local Area Network**
  VLAN's zijn de meest eenvoudige en flexibele manier om verkeer en gebruikers te scheiden op netwerken. De basisnetwerken van Constant IT hebben meestal een scheiding tussen VoIP verkeer en normaal verkeer maar in grotere netwerken kunnen meer VLAN's noodzakelijk zijn. Apparaten in de P2 en P3 categorie moeten de optie hebben om VLAN's aan te maken maar apparaten in de P1 categorie hoeven alleen het verkeer te kunnen onderscheiden (VLAN-tagging)

[5] http://www.networkmanagementsoftware.com/snmp-tutorial

VLAN verspreiding (VTP/GVRP)
In grote netwerken is het wenselijk om VLANS automatisch te laten verspreiden, op deze wijze wordt veel tijd bespaart bij het instellen van switches en zijn de VLANs overal hetzelfde. Er bestaan verschillende protocollen waarmee dit bereikt kan worden, één daarvan is het VTP (VLAN Trunking Protocol)
VTP is een Cisco protocol dat de VLAN informatie verspreid over verschillende switches in een VTP domein. Het wordt gebruikt om de VLAN informatie gelijk te houden binnen het domein en is vooral nuttig wanneer er veel VLANs en switches zijn in de omgeving. Van dit protocol bestaan uiteraard ook varianten bij alle andere fabrikanten van switches. Zo gebruikt HP bijvoorbeeld het eigen GVRP protocol wat precies hetzelfde doet.

- **Security levels instellen**
  Security levels worden gebruikt om bepaalde gebruikers meer rechten te geven op de te beheren apparatuur. Zo zijn er altijd root users maar ook users die bijvoorbeeld alleen mogen kijken en geen wijzigingen kunnen doorvoeren.
  Constant IT wil graag ook een scheiding hebben tussen werknemers die wel instellingen mogen aanpassen op apparatuur en werknemers die dit niet mogen.
  Het minimaal wenselijke is het bestaan van een read/write account en een read-only account

- **ACL (Access Control List)**
  ACL's worden gebruikt om gebruikers toegang te geven of ontzeggen tot bepaalde bronnen op het netwerk. Switches kunnen op deze manier ook toegang regelen op een wijze dat routers dat ook doen. Switches die functioneren op layer 3 en in grote complexe infrastructuren staan kunnen gebruik maken van deze feature. Switches die op layer 2 functioneren kunnen dit niet maar daar worden ACL's geregeld door routers. . Zie ook de tekst onder hoofdstuk 3.4.5.

3.2.6 ONDERSTEUNING & FABRIKANT

	Ondersteuning	P1 (laag)	P2 (middel)	P3(hoog)
Must have	• Community	V	V	V
	• Helpdesk support	X	V	V
Should have	• Certificering & partnerships	V	V	V
Could have	• Training	X	V	V
Won't have				

Figuur 33 Eisen ondersteuning & fabrikant switches

- **Community**
  Constant IT wil dat een gekozen product mede gedragen wordt door een community of forum zodat daar eventueel antwoorden gevonden kunnen worden op vragen die men heeft.

- **Helpdesk support**
  Constant IT is een bedrijf met veel jonge werknemers waardoor soms de kennis tekort schiet. Hierdoor is het noodzakelijk om toegang te hebben tot ondersteuning vanuit de fabrikant. Er dient rekening gehouden te worden met het feit dat apparaten ook uitgefaseerd kunnen worden, dit houdt vaak in dat apparaten nadat ze EOL (End Of Life) zijn niet meer ondersteund worden. Er worden dus geen apparaten gebruikt die al uitgefaseerd worden.

- **Certificering & partnerships**
  Door certificeringen te behalen kan Constant IT het kennisniveau verhogen door middel van het behalen van toetsen. Bij sommige fabrikanten bestaat ook de mogelijkheid om partner te worden, dit hangt meestal aan een aantal eisen vast zoals bijvoorbeeld dat er certificaten aanwezig moeten zijn. Door partner te worden van een fabrikant zijn er meerdere voordelen te behalen zoals bijvoorbeeld lagere inkooprijzen wat leidt tot hogere marges voor Constant IT. Een ander voordeel is dat er sneller gereageerd wordt op support aanvragen.

- **Training**
  Constant IT wil graag het kennisniveau van alle werknemers op een hoog peil hebben waardoor trainingen gewenst zijn. Dit omvat trainingen op locatie of via het internet. Vaak hangen er aan de bovengenoemde certificeringen ook trainingen vast.

3.3.1 ROUTER/FIREWALLS

Dit hoofdstuk beschrijft de eisen en wensen van switches op zowel laag 2 als laag 3. De eisen en wensen zullen onder de tabellen uitgeschreven worden zodat er geen verwarring kan ontstaan of de inhoud. De routers en firewalls worden in één categorie vergeleken, dit is overlegd met Constant IT en de reden hiervoor is dat iedere firewall kan routeren.

3.3.2 Toekomstvastheid

Toekomstvastheid		P1 (laag)	P2 (middel)	P3(hoog)
Must have	• Mogelijkheid tot clustering	X	X	V
	• Multi wan (failover of bundelen)	V	V	V
	• Gigabit poorten	V	V	V
	• IPv6	V	V	V
	• Link aggregation	X	V	V
Should have				
Could have	• Uitbreidbaarheid via licenties	V	V	V
Won't have				

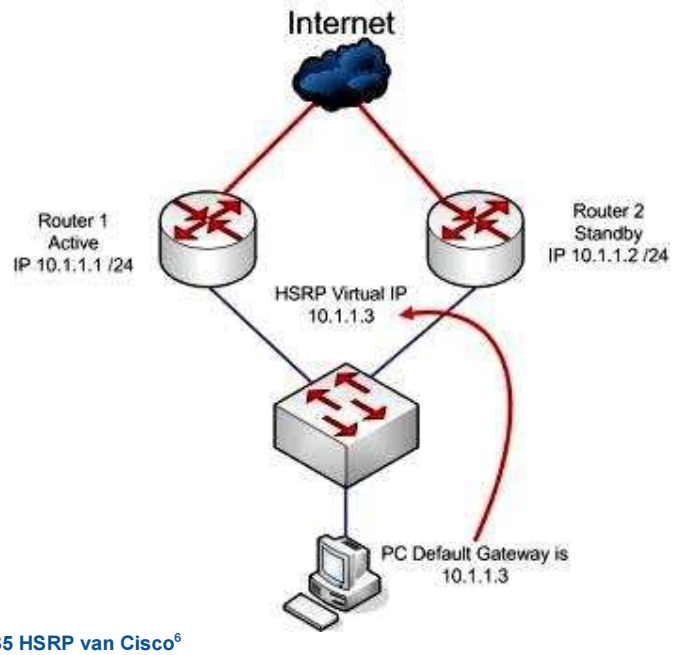
Figuur 34 Eisen toekomstvastheid routers en firewalls

- **Mogelijkheid tot clustering**
  Voor de snel groeiende klanten van Constant IT is het noodzakelijk dat er ondersteuning is voor het maken van een cluster. Een cluster is een groep apparaten die samen werken als één apparaat en gezamenlijk meer capaciteit hebben.

- **Multi WAN (network load balancing)**
  Constant IT heeft klanten die 24/7 zaken doen en dus verbinding moeten hebben met het internet. Daarom wordt er steeds vaker gekozen voor een oplossing die met meerdere WAN verbindingen tegelijk overweg kan. Deze oplossing kan op twee manieren geconfigureerd worden namelijk:

  - Failover
    Wanneer één WAN verbinding uitvalt, neemt de andere het over zodat er altijd internetverkeer mogelijk blijft.
    Wanneer de verbinding weer terug komt is het de bedoeling dat de primaire (snelle) verbinding weer als primaire lijn ingesteld wordt. Wanneer een link down gaat dient er ook een notificatie gestuurd te worden.

  - Load balancing
    In omgevingen met veel medewerkers, en dus veel connecties kan het handig zijn om via load balancing twee WAN verbindingen simultaan te gebruiken. Op deze manier wordt de bandbreedte sterk verhoogt doordat de snelheid van de WAN verbindingen in principe opgeteld kan worden. Echter is het zo dat individuele downloads niet sneller worden, een download loopt via één van de twee WAN verbindingen.



Figuur 35 HSRP van Cisco[6]

- **Gigabit poorten**
  Constant IT wil qua routers en firewalls gigabit apparatuur gaan leveren. Er staan op dit moment op veel locaties nog 100Mbit apparaten die in sommige gevallen een vertragende factor zijn. Constant IT streeft er na om alle netwerken bij alle klanten van gigabit snelheden te voorzien.

- **IPv6**
  Nieuwe apparatuur kan niet meer zonder IPv6 ondersteuning vanwege het op raken van de IPv4 adressen. Het is aannemelijk dat alle nieuwe hardware deze ondersteuning al ingebouwd heeft echter wordt de eis voor de zekerheid meegenomen
  (RIPE NCC, 2014)

- **Link aggregation**
  Het bundelen van interne verbindingen(LAN) wordt door Constant IT gebruikt zodat snelheid verhoogd kan worden. Met behulp van link aggregation kunnen snelheden richting bepaalde apparaten opgevoerd worden maar is er ook een vorm van redundantie aanwezig.

- **Uitbreidbaarheid via licenties**
  De Watchguard firewalls waar Constant IT ervaring mee heeft hebben een licentie model dat uitbreidbaar is. Zo kan er wanneer dit nodig is extra features aan de licentie toegevoegd worden. Voor de standaardisatie zou dit kunnen betekenen dat overal hetzelfde apparaat geleverd wordt met andere licenties.

[6] http://cn.cbsimg.net/cnwk.1d/i/tr/Jenna/Cisco_0405.jpg

3.3.3 Beheerbaarheid /beheerbaarheid

	Beheerbaarheid /betrouwbaarheid	P1 (laag)	P2 (middel)	P3(hoog)
Must have	• Loggen via webinterface, syslog of mail.	V	V	V
Should have	• Reporting op basis van vooraf ingestelde paramaters	X	V	V
	• Backup & Restore configuraties			
	• Console port aansluiting	X	V	V
	• Diagnostische tools	V	V	V
Could have	• Opties voor centraal beheer	X	X	V
Won't have	• Kaseya integratie	X	X	X

Figuur 36 Eisen beheerbaarheid routers en firewalls

- **Loggen via webinterface, syslog of mail.**
  Het is noodzakelijk dat Constant IT weet wat er speelt op de apparatuur van klanten waardoor er behoefte is naar een vorm van logging. Logging kan gebruikt worden om oorzaken van problemen terug te vinden of om preventief problemen aan te pakken. Het apparaat kan het zelf bijhouden en zichtbaar maken maar eventueel zijn er ook opties om dit centraal te doen.

- **Reporting op basis van vooraf ingestelde paramaters**
  Constant IT wil graag op basis van vooraf gedefinieerde parameters zaken kunnen loggen ten behoeve van reporting. Dit betreft dus het verzamelen van data voor een management summary en technische audit. Hetgeen dat minimaal te zien moet zijn is:

  - WAN bandbreedte
  - VPN bandbreedte

  Voor bovengenoemde aspecten geldt dat in ieder geval de volgende zaken meetbaar zijn/zijn in te stellen:
  - Throughput van de interface (MB)
  - Transfer amount van de interface (Mbps)
  - Mogelijkheid tot aanpassen tijdspanne van de verzamelde informatie (werkuren, dag, week en maand)
  - Overzicht grootgebruikers
    - client transfer amount
    - destination transfer amount

- **Console port aansluiting**
  Constant IT wil dat apparaten een console aansluiting hebben zodat er op locatie eenvoudig via een console cable op het apparaat geconfigureerd kan worden. Dit om te voorkomen dat men buitengesloten kan worden door misconfiguraties en/of storingen.

- **Diagnostische tools**
  Voor apparaten is het zeer wenselijk dat er “tools” aan boord zijn waarmee troubleshooting uitgevoerd kan worden. Voorbeelden zijn mogelijkheden tot debugmodus, maken van analyses en eenvoudige tools om connectiviteit te testen zoals ping.

- **Opties voor centraal beheer**
  Om het beheer te vereenvoudigen zou Constant IT graag willen dat apparaten opties hebben om naar een server te verbinden voor het beheer.
  - Management suite waarmee meerdere apparaten van hetzelfde merk beheerd kunnen worden in één centrale locatie
  - Deployment suite waarmee installaties naar apparaten kunnen worden verstuurd.

- **Kaseya integratie**
  Een eerder afstudeer stagiair heeft onderzoek gedaan naar de mogelijkheid om Kaseya informatie te laten opvangen van netwerkapparatuur. Destijds bleek dit onmogelijk. Omdat de functionaliteiten niet aanwezig zijn vanuit Kaseya hoeft er in deze vergelijking geen rekening gehouden te worden met integratie.

3.3.4 FEATURES

Features		P1 (laag)	P2 (middel)	P3(hoog)
Must have	• Site to site VPN	V	V	V
	• Voldoende VPN troughput	V	V	V
	• VPN failover	X	V	V
	• Qos & Traffic management/shaping	V	V	V
	• Policy based traffic management (ACL)	X	X	V
	• DHCP	V	V	V
	• SNMP	V	V	V
	• Verschillende NAT types (specifiek NAT loopback)	V	V	V
Should have	• LDAP/AD integratie	X	V	V
	• Modem functionaliteit	V	V	V
Could have				
Won't have				

Figuur 37 Eisen features routers en firewalls

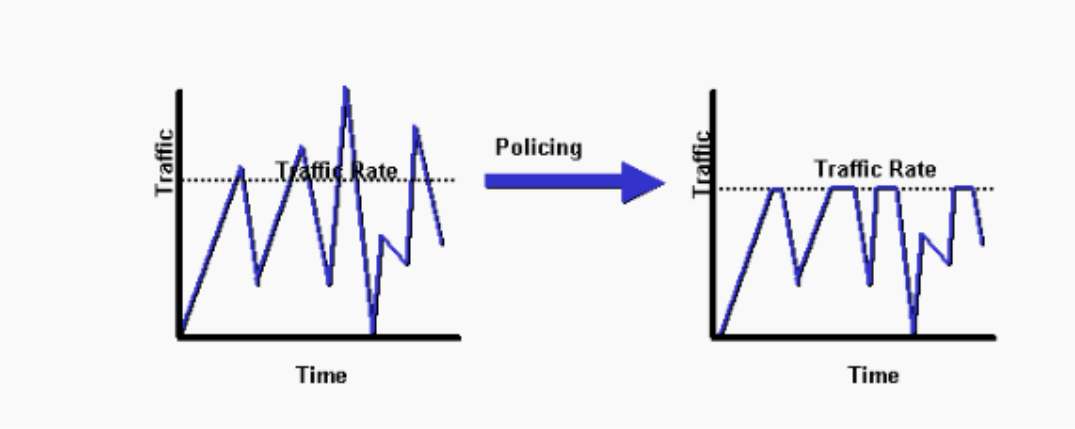
- **Site to Site VPN (Virtual Private Network)**
  Een Site to Site VPN is een tunnel methode waarbij de verschillende clients geen losse VPN software op hun computer hoeven te installeren. In plaats daarvan wordt de VPN opgebouwd tussen de routers/firewalls. Constant IT ziet dit als een must have eis omdat dit een oplossing is waar klanten niets van zien. Door het gebrek aan losse software kan er weinig misgaan wanneer hiermee gewerkt wordt.

- **Voldoende VPN troughput**
  Om te kunnen garanderen dat werknemers bij klanten via VPN een snelle verbinding hebben moet een apparaat voldoende VPN troughput hebben. In de bijlage zijn er VPN bandwidth reports te vinden. Deze reports zijn gemaakt over een werkdag zodat er een goed beeld ontstaat van de benodigdheden. De reports wijzen echt eruit dat er gedurende de dag dermate weinig VPN verkeer over de lijn loopt dat vrijwel elk apparaat zal voldoend hieraan. De hoogste piek in de reports is ongeveer 10Mbit.

- **VPN failover**
  Onder VPN failover verstaat Constant IT het maken van een tunnel op de loopback interfaces van een firewall/router. Loopback interfaces kunnen niet "down" gaan waardoor er in het geval van een dual-wan opstelling altijd toegang tot de tunnel is. Anderzijds mag/kan dit ook opgelost worden met route tables.

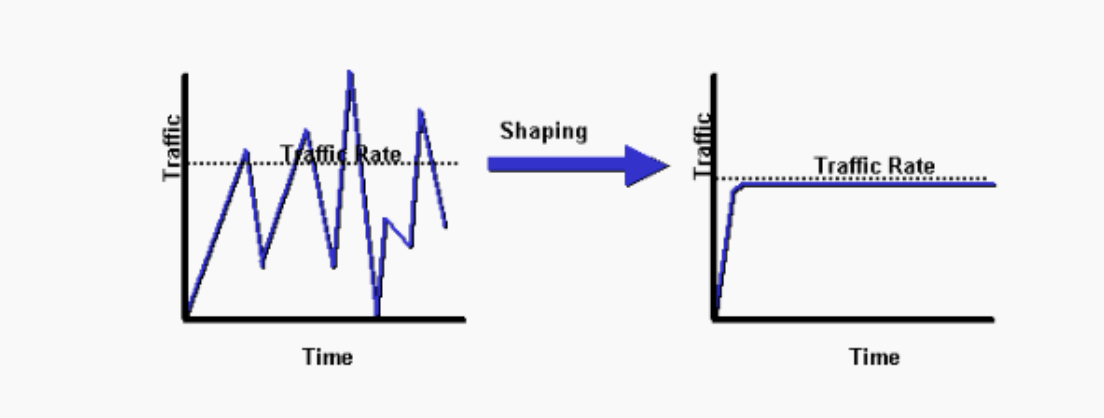
- **QoS (Quality of Service)**
  Quality of Service zorgt er voor dat bepaalde services binnen een netwerk gegarandeerd worden door middel van prioritering. Er zou bijvoorbeeld gekozen kunnen worden om VoIP verkeer hogere prioriteit te geven waardoor er geen pakketten wegvallen en de service altijd stabiel blijft draaien. Constant IT verstaat onder QoS de aanwezigheid van “traffic policing” en/of “traffic shaping”.(Cisco, 2005)

    - **Traffic policing**
      Dit is de term die door Cisco gebruikt wordt voor de meest eenvoudige vorm van QoS. Met deze methode wordt er een limiet ingesteld op een vorm van verkeer, wanneer deze limiet wordt gepasseerd worden er TCP/IP pakketten gedropt. Deze methode van QoS voorziet wel in het garanderen van bepaald verkeer maar tegen de prijs dat ander verkeer mogelijk niet aan komt. Traffic policing werkt op zowel inkomend als uitgaand verkeer.



Figuur 38 Traffic policing

    - **Traffic shaping**
      Traffic shaping is een methode waarin in een wachtrij wordt gebruikt, wanneer de limiet bereikt is worden TCP/IP pakketten in de wachtrij gezet. Pakketten in de wachtrij worden verstuurd volgens een schema, dit schema dicteert in welke pakketten geprioriteerd worden. Het nadeel van deze methode is dat er voldoende geheugen aanwezig moet zijn om een wachtrij te faciliteren.



Figuur 39 Traffic shaping

- **Policy based traffic management (ACL)**
  ACL's zijn een manier om gebruikers en groepen toegang te geven of ontzeggen tot aan het netwerk gekoppelde apparaten. Door permissies op een slimme wijze te gebruiken wordt de beveiliging verbeterd en de snelheid van het netwerk verhoogd.

- **DHCP (Dynamic Host Configuration Protocol)**
  Dit protocol dat al jaren gebruikt wordt om PC's een IP adres te geven moet ook aanwezig zijn op de door Constant IT geleverde apparaten.

- **SNMP (Simple Network Management Protocol)**
  SNMP is een protocol dat helpt bij het beheer van vrijwel alle apparaten van netwerkapparatuur tot aan servers. SNMP is al jaren een standaard op het gebied van management en Constant IT wil dat alle aangekochte apparaten dit protocol ondersteunen. Tevens kan er op een later moment gepoogd worden om devices met het interne gebruikte systeem (Kaseya) te koppelen om devices te monitoren en managen

- **Verschillende NAT(Network Address Translation) typen. (specifiek NAT loopback)**
  Constant IT eist van routers/firewalls dat ze in alle gangbare NAT versies kunnen voorzien. Daarnaast bestaat de wens dat apparaten ook kunnen voorzien in Loopback NAT wat er voor zorgt dat externe IP adressen vanaf het interne netwerk bereikbaar zijn.

- **LDAP/AD integratie (radius)**
  Constant IT wil graag overal de wachtwoorden en gebruikersnamen hetzelfde houden. Het is daarom het meest praktisch om zoveel mogelijk integreren met het Active Directory van de Windows servers. Het radius protocol wordt, hoewel het al vrij oud is nog steeds verder ontwikkeld.

- **Modem Functionaliteit**
  Bij klanten van Constant IT is het nu zo dat er een modem staat van de provider en daarachter komt pas de firewall van Constant IT. Dit modem doet eigenlijk niets behalve verkeer doorgeven omdat hij ingesteld is als een "bridge". Echter kan dit modem wel kapot gaan. Constant IT wil graag een firewall of router die ook direct aan een DSL lijn verbonden kan worden.

3.3.5 VEILIGHEID

	Veiligheid	P1 (laag)	P2 (middel)	P3(hoog)
Must have	• IPsec	X	V	V
	• VLAN support	V	V	V
	• ACL's	X	V	V
Should have	• Proxy support / Web filtering.	X	X	V
	• DDOS herkenning.	X	V	V
Could have	• IDS/IPS	X	V	V
	• Security levels instellen	X	V	V
	• Audit logs	X	V	V
Won't have				

Figuur 40 Eisen veiligheid routers en firewalls

- **IPSec**
  IPSec is een protocol dat gebruikt wordt om VPN verbindingen te beschermen tegen onder andere aanvallen op de VPN verbinding, data corruptie, data diefstal. IPsec beschermt data integriteit, vertrouwelijkheid en authenticiteit. (Microsoft , 2003)

- **VLAN support**
  Omdat de switches met VLANs werken is het noodzakelijk dat ook de routers/firewalls dit verkeer kunnen onderscheiden.

- **ACL's (Access Control Lists)**
  ACL's zijn filters die de mogelijkheid bieden bepaalde types verkeer toe te staan of te weigeren naar bepaalde locaties in het interne netwerk. Een router die een pakket binnen krijgt houdt dit pakket eerst tegen de gedefinieerde ACL's om een beslissing te maken.

- **Proxy / webfiltering**
  Een proxy server is een server die als tussenpersoon functioneert voor client aanvragen. Een client verbind met de proxy server om een service op te vragen (webpagina, bestand). De proxy server evalueert aanvragen. Tegenwoordig zijn de meeste proxyservers web proxies wat betekend dat ze internet toegang faciliteren en anonimiteit verschaffen op het internet.

  Constant IT zou graag willen dat apparaten ook de mogelijkheid hebben om als proxy server te functioneren zodat internet toegang centraal beheerd kan worden. Constant IT wil graag dat proxy instellingen te forceren zijn waardoor gecontroleerd kan worden wat gebruikers doen op het internet. Wanneer de klant de wens heeft om bepaalde sites ontoegankelijk te maken is het fijn als apparatuur in deze wens kan voorzien met behulp van web filtering. Tevens houden proxy servers logboeken bij voor de gebruikers en statistieken voor het meten van bandbreedte. Er dienen ook notificaties gestuurd worden van het herhaaldelijke schendingen van de webfiltering.

- **DDOS (Distributed Denial Of Service) herkenning.**
  DDOS aanvallen zijn een groeiend probleem voor IT organisaties overal ter wereld. Zelfs de grootste bedrijven hebben problemen om deze aanvallen succesvol te bestrijden (ING Nederland, 2013).
  Hoewel echte DDOS aanvallen simpelweg heel veel legitieme pakketten sturen waardoor de lijn als het ware volloopt of via een specifieke methode die misbruikt maakt van een lek.
  Constant IT wil dat apparaten ten minste “well known” DDOS aanvallen kunnen detecteren en eventueel automatisch kunnen oplossen.

- **IDS/IPS (Intrusion Detection System / Intrusion Prevention System)**
  Beveiliging wordt steeds belangrijker omdat aanvallers steeds slimmer worden, Constant IT wil graag dat apparaten een manier hebben om aanvallen te voorkomen.
  Hiervoor wordt er gekeken naar Intrusion Detection Systems en Intrusion Prevention Systems.
  - Intrusion detection is een passief systeem dat incidenten logt en meldingen verstuurd naar de systeembeheerder. Het systeem kan ook helpen met het vinden van zwakheden en het vaststellen van problemen.

  - Intrusion prevention is een actief systeem dat verkeer controleert terwijl het binnen komt en aanvallen meteen afslaat. IPS kan besluiten om sessies of zelfs netwerkverbindingen te verbreken. Meer geavanceerde IPS kunnen ook attachments die als virus gezien worden deleten of zelfs patches op client uitvoeren om bepaalde zwakheden te beschermen.
    (Compare Business Products, 2014)

- **Security levels instellen**
  Security levels worden gebruikt om bepaalde gebruikers meer rechten te geven op de te beheren apparatuur. Zo zijn er altijd root users maar ook users die bijvoorbeeld alleen mogen kijken en geen wijzigingen kunnen doorvoeren.
  Constant IT wil graag ook een scheiding hebben tussen werknemers die wel instellingen mogen aanpassen op apparatuur en werknemers die dit niet mogen.
  Het minimaal wenselijke is het bestaan van een read/write account en een read-only account.

- **Audit logs**
  Audit logging is het monitoren van de acties die uitgevoerd zijn op een apparaat. Op deze manier kunnen incidenten worden reconstrueert omdat er op te vragen valt wat er gebeurd is. Daarnaast is het mogelijk om te zien wie iets heeft ingesteld waardoor werknemers aansprakelijk gesteld kunnen worden voor eventuele fouten.

3.3.6 ONDERSTEUNING & FABRIKANT

	Ondersteuning	P1 (laag)	P2 (middel)	P3(hoog)
Must have	• Community	V	V	V
	• Helpdesk support	X	V	V
Should have	• Certificering & partnerships	V	V	V
Could have	• Training	X	V	V
Won't have				

Figuur 41 Eisen ondersteuning & fabrikant routers en firewalls

- **Community**
  Constant IT wil dat een gekozen product ondersteund wordt door een community of forum zodat daar eventueel vragen en antwoorden gevonden kunnen worden wanneer er complexe incidenten zijn.

- **Helpdesk support**
  Constant IT is een bedrijf met veel jonge werknemers waardoor soms de kennis tekort schiet. Hierdoor is het niet gewenst om zelf het hoogste niveau van support te zijn en moet er naar alternatieven worden gekeken bij de fabrikanten. Veel fabrikanten leveren tegen een meerprijs extra support op hun producten en Constant IT wil daar gebruik van maken als dat verantwoord is. Er dient rekening gehouden te worden met het feit dat apparaten ook uitgefaseerd kunnen worden, dit houdt vaak in dat apparaten nadat ze EOL (End Of Life) zijn niet meer ondersteund worden. Er worden dus geen apparaten gebruikt die al uitgefaseerd worden.

- **Certificering & partnerships**
  Door certificeringen te behalen kan Constant IT partner worden van bepaalde fabrikanten en een hoger kennisniveau behalen omdat er vaak trainingen aan vast zitten. Deze partnerships kunnen dan weer leiden tot lagere inkoopprijzen en dus hogere marges.

- **Training**
  Constant IT wil graag het kennisniveau van alle werknemers op een hoog peil hebben waardoor trainingen gewenst zijn. Dit omvat trainingen op locatie of via het internet.

4 ERVARINGEN

Dit hoofdstuk beschrijft de ervaringen die Constant IT heeft met recent geleverde apparaten. De informatie in dit hoofdstuk is gebaseerd op de informatie die verkregen is via interviews met de Service Development en Service Execution afdelingen. De ervaringen van de verschillende medewerkers zijn uiteindelijk relevant in de vergelijking omdat producten en/of fabrikanten waar goede ervaringen mee zijn bonuspunten krijgen.
Door middel van een gesprek met de sales afdeling is achterhaalt welke apparaten het meest verkocht zijn dit jaar. In de tabel hieronder worden de apparaten die dit jaar exclusief geleverd zijn weergegeven.

Routers	Firewalls	Switches L2	Switches L3
Draytek 2130	Watchguard XTM 26	Netgear GS108	Cisco Catalyst 2960
Draytek 2925Vn+	Watchguard XTM 26	Cisco SG200	
	Watchguard XTM33	Cisco SG300	

Figuur 42 Meest geleverde apparaten Constant IT

In de pagina's hieronder worden de resultaten van de afgenomen interviews beschreven, de vragen bestaan veelal uit open vragen en een enkele gesloten vraag. De complete interviews zijn te vinden in bijlage 1.

Algemeen
Uit de interviews is gebleken dat er bij vrijwel alle klanten een Draytek router of een Watchguard firewall die ook als router kan functioneren wordt geleverd. Voor switches worden er bijna altijd Netgear, HP of Cisco switches geleverd. Dit valt ook terug te zien in de ervaringen. De algemene impressie is wel dat er nooit slechte apparatuur geleverd wordt

Switches layer 2
De Netgear unmanaged switches worden intern gebruikt om meer aansluitingen te krijgen, deze 8 poort switches zijn echter zeer stabiel, zelfs in een omgeving waar veel van ze gevraagd wordt. De HP Procurves en Cisco SG / Catalyst switches bevinden zich bij klanten maar hebben eigenlijk nooit problemen, zijn relatief eenvoudig in te stellen via de webinterface of CLI en hebben een goede performance.
Er bestaan echter ook negatieve ervaringen met de HP Procurves, specifiek het 1800 model. Deze instapmodellen maken gebruik van een Java plug-in om he apparaat te benaderen en dit functioneert niet geweldig, daarnaast staat JAVA niet bekend als waterdicht wat ook veiligheidszorgen met zich mee brengt. De HP Procurves hadden ook problemen met het maken en gebruiken van VLAN's.
Van switches van TP-Link wordt gezegd dat deze niet in de organisatie thuishoren in verband met de algehele kwaliteit die niet voldoende is.

Switches layer3
Onder de layer 3 routers is het alleen Cisco dat de klok slaat onder de werknemers van Constant IT. De producten worden geroemd om hun stabiliteit, de Cisco's hoeven maar eenmalig geconfigureerd te worden om er vervolgens niet meer naar om te hoeven kijken. Switches op layer 3 worden echter zelden verkocht en er zijn niet veel ervaringen mee.

Routers
Draytek routers worden vooral ingezet bij de kleinere klanten die alleen basisfunctionaliteit nodig hebben. In de interviews worden deze apparaten genoemd als passend of voldoende maar niet als bovengemiddeld goed. Bij grotere klanten wordt eigenlijk altijd een all-in-one oplossing gebruikt in de vorm van een Watchguard, meer hierover onder het kopje firewalls. Er staat ook een aantal overgenomen Zyxel routers maar deze voldoen niet aan de verwachte eisen die men stelt aan stabiliteit en bouwkwaliteit. Er zijn zelfs ervaringen met Zyxels die doorgebrand zijn.

Firewalls
Als beste firewall oplossing wordt door eigenlijk alle werknemers Watchguard genoemd. Deze apparaten worden sinds een tijd als all-in-one oplossing bij klanten neergezet. De Watchguard firewalls worden ervaren als goed en er is veel ervaring met deze apparatuur. Echter zijn er ook collega's die de VPN stabiliteit niet voldoende vinden en dat de apparaten te vaak herstart moeten worden. Er bestaan ook ervaringen met Fortigate, wat een directe concurrent van Watchguard is maar deze zijn veelal negatief. De interface voelt niet goed aan en de apparaten zijn instabiel, de vraag is tot in hoeverre dit gerelateerd is tot het beperkte kennisniveau.

Support
In de interviews wordt HP vooral geroemd om de snelle service die te verkrijgen valt met behulp van Care Packs. Wanneer er echt een probleem is staat HP de volgende werkdag op de stoep met een monteur die eventueel het apparaat vervangt. Cisco wordt aan de andere kant geroemd vanwege de bekendheid die het merk heeft waardoor problemen eenvoudig te troubleshooten zijn. Daarnaast kent Cisco ook next business day support en hebben ze een helpdesk die benaderd kan worden. Voor beide merken geldt dat aan deze kwaliteit wel een prijskaartje hangt, dit is bekend en vormt naar de mening van de geïnterviewde personen geen probleem.
De ervaringen met Watchguard support zijn neutraal, de doorlooptijden zijn behoorlijk traag waardoor problemen meestal al opgelost zijn voordat er bij Watchguard geëscaleerd wordt.

4.1 UITWERKING INTERVIEWS IN NUMMERS

Op de volgende pagina staat een tabel waarmee aangegeven wordt welke werknemers dezelfde apparaten positief benoemden. Op deze manier valt er een lijn te trekken naar welke apparaten wenselijk zijn. Om te achterhalen hoe wenselijk apparaten van een bepaald type, merk of fabrikant zijn wordt er een berekening gedaan. Hieronder een voorbeeld berekening

Product X heeft 4 ervaringen uit 10 interviews, dit betekend dat de bekendheid van het product 40% is. Omdat er 4 ervaringen zijn telt elke ervaring voor 25% mee bij het optellen van de wenselijkheid.
Er zijn 2 positieve ervaringen, deze tellen gezamenlijk voor 50%.
Er is 1 neutrale ervaring, deze telt 12.5% mee bij het optellen, de overige 12.5% wordt als het ware opgeteld bij de negatieve kant.
Er is 1 negatieve ervaring, deze heeft geen procentuele waarde. Door de ervaringen op te tellen (25%+25%+12.5%) wordt er uitgekomen op 62.5% wenselijkheid.

Constant IT

Legenda

+	Positief
=	Neutraal
-	Negatief
Bekendheid	Dit kopje geeft aan hoeveel procent van de werknemers een noemenswaardige ervaring hebben met dit product
Wenselijkheid	Dit kopje geeft aan hoe wenselijk een bepaald product is in de organisatie gebaseerd op de ervaring (zowel positief als negatief)

Merk/Serie/Fabrikant	Type	Bilal	Gerrit	Bas	Barry	Jan-Kees	Maurits	Niels	Kilian	Robin	Thierry	Positief	Neutraal	Negatief	Aantal ervaringen	Aantal zonder ervaring	Bekendheid	Wenselijkheid
Netgear 108 serie	SWL2	+	X	+	X	X	X	X	X	+	+	4	0	0	4	6	40%	100%
HP procurve series	SWL2	+	X	-	X	X	+	X	X	X	X	2	0	1	3	7	30%	66.6%
Cisco SG series	SWL2	X	+	+	+	X	X	+	X	X	+	6	0	0	6	4	60%	100%
TP-Link switches	SWL2	X	X	X	X	X	X	X	-	X	X	0	0	1	1	9	10%	0%
Cisco catalyst 26xx	SWL3	+	+	X	X	+	X	X	X	X	+	4	0	0	4	6	40%	100%
Cisco catalyst 37xx	SWL3	X	X	X	X	X	+	+	X	X	X	1	0	0	1	9	10%	100%
Draytek	R	+	X	X	X	X	-	=	=	+	+	3	2	1	6	4	60%	66.4%
Cisco 2901	R	+	X	X	X	X	X	X	+	X	X	2	0	0	2	8	20%	100%
Zyxel	R	X	X	X	X	X	-	X	X	X	X	0	0	1	1	9	10%	0
Watchguard	FW	=	-	+	=	X	+	+	X	+	X	4	2	1	7	3	70%	71.4%
Cisco ASA	FW	X	X	=	X	X	X	X	X	X	X	0	1	0	1	9	10%	50%
Fortigate	FW	X	X	X	X	-	X	X	X	X	X	0	0	1	1	9	10%	0
												4						
HP	Support	+	+	X	X	X	+	+	+	X	+	6	0	0	6	4	60%	100%
Cisco	Support	X	X	+	+	X	X	+	+	X	X	4	0	0	4	6	40%	100%
Watchguard	Support	X	X	=	X	+	X	X	X	X	X	1	1	0	2	8	20%	75%

Figuur 43 Overzicht resultaten interviews

FIGURENLIJST

Figuur 21 Verdeling klanten Constant IT 6
Figuur 22 Prijsindeling routers/firewalls 7
Figuur 23 Prijsindeling switches 7
Figuur 24 Indeling hoeveelheid gebruikers 7
Figuur 25 Switchpoorten 7
Figuur 26 Voorbeeld stackable switch 8
Figuur 27 Eisen toekomstvastheid switches 10
Figuur 28 SFP+ 10 GE expansion van HP 11
Figuur 29 Eisen beheerbaarheid switches 12
Figuur 30 Eisen features switches 14
Figuur 32 Eisen veiligheid switches 15
Figuur 33 Eisen ondersteuning & fabrikant switches 17
Figuur 34 Eisen toekomstvastheid routers en firewalls 18
Figuur 35 HSRP van Cisco 19
Figuur 36 Eisen beheerbaarheid routers en firewalls 20
Figuur 37 Eisen features routers en firewalls 22
Figuur 38 Traffic policing 23
Figuur 39 Traffic shaping 23
Figuur 40 Eisen veiligheid routers en firewalls 25
Figuur 41 Eisen ondersteuning & fabrikant routers en firewalls 27
Figuur 42 Meest geleverde apparaten Constant IT 28
Figuur 43 Overzicht resultaten interviews 30

REFERENTIES

Cisco. (2005, Augustus 10). *Quality of service - Difference between policing and shaping.* Retrieved from Cisco: http://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html#policingvsshaping

Compare Business Products. (2014, 3 18). *Security: IDS vs. IPS Explained*. Retrieved from http://www.comparebusinessproducts.com/: http://www.comparebusinessproducts.com/fyi/ids-vs-ips

ING Nederland. (2013, 4 5). *Achtergronden storingen banken*. Retrieved from ING.nl: https://www.ing.nl/nieuws/nieuws_en_persberichten/2013/04/Achtergronden_storingen_banken.aspx?first_visit=true

International Institute of Buisiness Analysis. (2009). *a guide to the business analysis body of knowledge (babok guide)* . Retrieved from http://www.iowadnr.gov/: http://www.iowadnr.gov/portals/idnr/uploads/Iowa%20Outdoors%20News/2011/BABOK%20Version2.pdf

Microsoft . (2003, 03 28). *What Is IPSec?* Retrieved from Microsoft Technet: http://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx

Paul Congdon, I. (02, 7 3). *Link Layer Discovery*. Retrieved from http://www.ieee802.org/: http://www.ieee802.org/1/files/public/docs2002/lldp-protocol-00.pdf

Rajesh, K. (2012, May 25). *What is LLDP (Link Layer Discovery Protocol)?* Retrieved from excITingIP.com: http://www.excitingip.com/3026/what-is-lldp-link-layer-discovery-protocol/

RIPE NCC. (2014, 6 24). *Reaching the last /8*. Retrieved from www.ripe.net: http://www.ripe.net/internet-coordination/ipv4-exhaustion/reaching-the-last-8

Schellevis, J. (2012, 9 14). *RIPE NCC deelt laatste blok ipv4-adressen uit*. Retrieved from Tweakers: http://tweakers.net/nieuws/84386/ripe-ncc-deelt-laatste-blok-ipv4-adressen-uit.html

Steehouder, M. (2012). *Leren Comminuceren.* Noordhoff Uitgevers B.V.

TOGAF. (2011). *Togaf 9.1 overview*. Retrieved from togaf.com: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap37.html

BIJLAGE 1 INTERVIEW SERVICE DEVELOPMENT & SERVICE EXECUTION

SERVICE DEVELOPMENT

Vraag	Antwoord		
Naam	Bilal El Haddouchi		
Functie:	Technical Specialist Service Development		
Welke hardware heb je geconfigureerd na 2012, (switches, firewalls routers?)	Switch	Router	Firewall
	X	X	X
Beschrijf kort je rol binnen Constant IT.	Dagelijkse werkzaamheden bij constant IT zijn zeer variërend maar ik hou me vooral bezig met netwerkbeheer en serverinstallatie/beheer.		
Met welke hardware fabrikanten heb je ervaring?	Cisco (catalyst en small business varianten), Cisco routers (CLI), HP procurve switches via CLI. Watchguard XTM firewalls. Drayteks, Vigor 28xx. Basis Linksys apparatuur. Verschillende merken die wij overgenomen hebben van eerdere leveranciers zoals Zyxel en Fortigate		
Welke certificeringen/trainingen op het gebied van netwerkapparatuur heb je?	Cisco CCNA 1,2 ,3 en 4.		
Hoe schat je je kennis niveau op het gebied van netwerkapparatuur. (op een schaal van 1 t/m 5, waarin 1 geen kennis is en 5 een zeer hoog niveau)	Switch	Routers	Firewalls
	5	5	4
Zou je meer ervaring met netwerkcomponenten willen opdoen? (Zo ja, op welke gebieden)	Ja, in de niet al te nabije toekomst.		
Constant IT heeft veel verschillende hardware van veel verschillende fabrikanten, Welke fabrikant is volgens jou het beste, en waarom?	Watchguard, hier kunnen we goed mee uit de voeten. Hp en/of Cisco voor switches. (Mijn voorkeur gaat uit naar het Catalysts.)		
Welke switch (layer 2) (in ons assortiment) is naar jouw mening het beste, en waarom?	Unmanaged netgear switches of die van HP (bij voorkeur HP)		
Welke switch (layer 3) (in ons assortiment) is naar jouw mening het beste, en waarom?	Cisco Catalyst, na installatie geven deze nooit problemen.		
Welke router (in ons assortiment) is naar jouw mening het beste, en waarom?	Cisco routers, en Draytek voor de low end klanten.		
Welke firewall (in ons assortiment) is naar jouw mening het beste, en waarom?	De Watchguards zijn prima, we weten hoe het werkt. Als we naar een andere type zouden overstappen zouden we eerst ervaring hiermee moeten opbouwen.		
Welke fabrikant levert volgens u de beste support, en waarom?	HP, next business day apparatuur levering. Bij HP is er levenslange garantie op switches.		
Welke netwerkapparatuur die wij geleverd hebben vind je ronduit slecht, en waarom? (switch, router, firewall, merk)	Ik ben van mening dat wij goede apparaten leveren. Op dit moment hebben we wel wat issues met Watchguards maar ik ben niet van mening dat het apparaat slecht is.		
Wat mis je qua functionaliteiten/performance/etc. aan de huidige gebruikte producten/technologieën	Het gecentraliseerd beheren van alle klant routers. Vanuit één management console alle routers beheren.		
Als er nog dingen zijn die je wil toevoegen dan kan dat in dit hier.	Als je bijvoorbeeld een Watchguard plaats ben je meer uren kwijt aan het onderhoud dan bij een Cisco, daar heb je geen omkijken na.		

Vraag	Antwoord		
Naam	Gerrit Zwart		
Functie:	Technical Specialist Service Development		
Welke hardware heb je geconfigureerd na 2012, (switches, firewalls routers?)	Switch	Router	Firewall
	X	X	X
Beschrijf kort je rol binnen Constant IT.	Het onderzoeken van 2de lijns problemen en onderzoeken naar verbeteringen bij huidige en nieuwe klanten.		
Met welke hardware fabrikanten heb je ervaring?	Draytek, Linksys, Watchguard en HP.		
Welke certificeringen/trainingen op het gebied van netwerkapparatuur heb je?	CCNA exploration		
Hoe schat je je kennis niveau op het gebied van netwerkapparatuur. (op een schaal van 1 t/m 5, waarin 1 geen kennis is en 5 een zeer hoog niveau)	Switch	Routers	Firewalls
	3	3	3
Zou je meer ervaring met netwerkcomponenten willen opdoen? (Zo ja, op welke gebieden)	Ja graag, vooral op cisco gebied.		
Constant IT heeft veel verschillende hardware van veel verschillende fabrikanten, Welke fabrikant is volgens jou het beste, en waarom?	HP		
Welke switch (layer 2) (in ons assortiment) is naar jouw mening het beste, en waarom?	De SG serie van Cisco of de ooit eens geleverde netgears.		
Welke switch (layer 3) (in ons assortiment) is naar jouw mening het beste, en waarom?	De Cisco Catalyst 26XX		
Welke router (in ons assortiment) is naar jouw mening het beste, en waarom?	Watchguard XTM 26 bij gebrek aan beter.		
Welke firewall (in ons assortiment) is naar jouw mening het beste, en waarom?	Watchguard XTM 26 bij gebrek aan beter.		
Welke fabrikant levert volgens u de beste support, en waarom?	HP vanwege de snelle afhandeling van garantie issues.		
Welke netwerkapparatuur die wij geleverd hebben vind je ronduit slecht, en waarom? (switch, router, firewall, merk)	Dit is afhankelijk van de omgeving van de klant en het doel van het apparaat. Wij leveren geen slechte apparaten maar soms misplaatsen wij wel eens een apparaat.		
Wat mis je qua functionaliteiten/performance/etc. aan de huidige gebruikte producten/technologieën	Een goede, stabiele VPN omgeving. (site-to-site, dial-in)		
Als er nog dingen zijn die je wil toevoegen dan kan dat in dit hier.	Veel IT partners werken met HP + Cisco, daar valt ook wel wat voor te zeggen.		

Vraag	Antwoord		
Naam	Bas de Zeeuw		
Functie:	Technical Specialist Service Development		
Welke hardware heb je geconfigureerd na 2012, (switches, firewalls routers?)	Switch	Router	Firewall
	X	X	X
Beschrijf kort je rol binnen Constant IT.	Netwerk en systeembeheerder.		
Met welke hardware fabrikanten heb je ervaring?	Watchguard firewalls, cisco switches, HP wireless		
Welke certificeringen/trainingen op het gebied van netwerkapparatuur heb je?	CCNA, Netgear certificaat		
Hoe schat je je kennis niveau op het gebied van netwerkapparatuur. (op een schaal van 1 t/m 5, waarin 1 geen kennis is en 5 een zeer hoog niveau)	Switch	Routers	Firewalls
	4	4	4
Zou je meer ervaring met netwerkcomponenten willen opdoen? (Zo ja, op welke gebieden)	Ja, in principe wel. Het leukste is het ontwerpen van een hele omgeving dus ik zou graag daar meer mee willen doen.		
Constant IT heeft veel verschillende hardware van veel verschillende fabrikanten, Welke fabrikant is volgens jou het beste, en waarom?	Cisco, want daar is veel informatie over bekend. Error codes zijn goed te vinden op internet. Watchguard firewalls zijn ook prima.		
Welke switch (layer 2) (in ons assortiment) is naar jouw mening het beste, en waarom?	Netgear,G105 of 108 l2 switches, deze staan onder ons bureau. Deze kunnen vlan's taggen en verder eigenlijk niets.		
Welke switch (layer 3) (in ons assortiment) is naar jouw mening het beste, en waarom?	Cisco sg300, dit zijn perfecte MKB switches. Er vallen dingen meer dingen in te stellen dan op de low end versies maar ze zijn niet zo duur als Catalysts.		
Welke router (in ons assortiment) is naar jouw mening het beste, en waarom?	Watchguard XTM 26		
Welke firewall (in ons assortiment) is naar jouw mening het beste, en waarom?	Watchguard. Een Cisco ASA kan ook maar de CLI is niet ideaal wanneer er honderden regels toegevoegd moeten worden		
Welke fabrikant levert volgens u de beste support, en waarom?	Watchguard eerste lijns support is op zijn zachts gezegd niet heel erg fijn. Daarnaast heb ik zelf meestal het probleem al achterhaald voordat het geëscaleerd wordt. Het feit dat Cisco een forum naast helpdesk support waarop ook antwoorden gevonden kunnen worden maakt dat zei het beste support leveren.		
Welke netwerkapparatuur die wij geleverd hebben vind je ronduit slecht, en waarom? (switch, router, firewall, merk)	HP procurve 1800 series, deze zijn te beheren via een tool die Java nodig heeft, dit werkt slecht. Vlans werken hierop ook niet altijd even goed.		
Wat mis je qua functionaliteiten/performance/etc. aan de huidige gebruikte producten/technologieën	Niet van toepassing Bas heeft al bijgedragen aan verzamelen requirements.		
Als er nog dingen zijn die je wil toevoegen dan kan dat in dit hier.	Ik zou graag zien dat iedereen minimaal een basis niveau van kennis heeft op het gebied van netwerken (CCNA Exploration)		

Vraag	Antwoord		
Naam	Barry Oudejans		
Functie:	Technical Specialist Service Development		
Welke hardware heb je geconfigureerd na 2012, (switches, firewalls routers?)	Switch	Router	Firewall
	X	X	X
Beschrijf kort je rol binnen Constant IT.	Ondersteunen van klanten bij dagelijks gebruik van machines maar ook ondersteunen bij storingen op het netwerk, internet verbindingen en servers. Ondersteunen van collega's (vraagbaak). Opbouwen van servers voor nieuwe omgevingen.		
Met welke hardware fabrikanten heb je ervaring?	HP, Dell, Watchguard, Draytek, Cisco, Apple etc (erg veel)		
Welke certificeringen/trainingen op het gebied van netwerkapparatuur heb je?	Niets.		
Hoe schat je je kennis niveau op het gebied van netwerkapparatuur. (op een schaal van 1 t/m 5, waarin 1 geen kennis is en 5 een zeer hoog niveau)	Switch	Routers	Firewalls
	2	4	4
Zou je meer ervaring met netwerkcomponenten willen opdoen? (Zo ja, op welke gebieden)	Ja, bezig met CCNA switching en routing om kennisgat op te vullen. Ik hoop uiteindelijk nog meer ervaring op te doen.		
Constant IT heeft veel verschillende hardware van veel verschillende fabrikanten, Welke fabrikant is volgens jou het beste, en waarom?	Cisco, stabiel, goed te configureren en geen omkijken naar. Niet 2 maal per maand de stekker eruit om te herstarten zoals we wel zien bij andere merken.		
Welke switch (layer 2) (in ons assortiment) is naar jouw mening het beste, en waarom?	SG500		
Welke switch (layer 3) (in ons assortiment) is naar jouw mening het beste, en waarom?	SG500		
Welke router (in ons assortiment) is naar jouw mening het beste, en waarom?	Watchguards in het algemeen, we leveren niet veel anders op het moment		
Welke firewall (in ons assortiment) is naar jouw mening het beste, en waarom?	Watchguards in het algemeen, we leveren niet veel anders op het moment		
Welke fabrikant levert volgens u de beste support, en waarom?	Xpertdata (leverancier Draytek) levert prima support. Geen ervaring met Watchguard, maar ik hoor van collega's dat het niet goed is. Geen ervaring met Cisco support		
Welke netwerkapparatuur die wij geleverd hebben vind je ronduit slecht, en waarom? (switch, router,firewall, merk)	Watchguard doet in principe wat het moet doen, maar soms heeft het rariteiten. BV :tunnels die uitvallen en door matige logging is het niet eenvoudig te achterhalen waardoor het mis gaat. Tevens wordt Watchguard ook bedoeld als ik spreek over apparaten die 2 maal per maand herstart moeten worden.		
Wat mis je qua functionaliteiten/performance/etc. aan de huidige gebruikte producten/technologieën	Vrij weinig, je gaat pas over functionaliteiten nadenken wanneer klanten bepaalde requirements hebben. Ik zelf mis niets. BV vroeger leverden we ook geen Cisco switches omdat daar geen behoefte aan was.		
Als er nog dingen zijn die je wil toevoegen dan kan dat in dit hier. (Hier staat ook informatie die buiten de vragen valt)	Soms leveren wij nog Drayteks als klanten op de centen moeten letten		

Vraag	Antwoord		
Naam	Jan Kees Kuiper		
Functie:	Technical Specialist SD		
Welke hardware heb je geconfigureerd na 2012, (switches, firewalls routers?)	Switch	Router	Firewall
	X	X	X
Beschrijf kort je rol binnen Constant IT.	Servers beheren, af en toe ben ik wel eens op basis niveau bezig met het configureren van netwerkapparatuur (vlans, exports, imports)		
Met welke hardware fabrikanten heb je ervaring?	Bijna geen ervaring op het gebied van configuratie want ik ben altijd server beheerder geweest, ik weet wel de theorie erachter.		
Welke certificeringen/trainingen op het gebied van netwerkapparatuur heb je?	Niets		
Hoe schat je je kennis niveau op het gebied van netwerkapparatuur. (op een schaal van 1 t/m 5, waarin 1 geen kennis is en 5 een zeer hoog niveau)	Switch	Routers	Firewalls
	2	2	2
Zou je meer ervaring met netwerkcomponenten willen opdoen? (Zo ja, op welke gebieden)	Ja, nadat server 2012 certificering behaald is. Ik wil graag wat meer all-round worden.		
Constant IT heeft veel verschillende hardware van veel verschillende fabrikanten, Welke fabrikant is volgens jou het beste, en waarom?	Cisco, want ze zijn goed gebouwd, hebben een inruilprogramma. Het is duur en maar je er valt wel te merken waarom. Voor goedkopere zaken, asus routers. Veel updates, top support. Het is wel plastic, maar werkt goed (genoeg).		
Welke switch (layer 2) (in ons assortiment) is naar jouw mening het beste, en waarom?	Het enige netwerk apparaat waar ik actief bij betrokken ben geweest is de Catalyst 2k. wij hebben deze al enige tijd geleden neergezet maar is nog nooit herstart.		
Welke switch (layer 3) (in ons assortiment) is naar jouw mening het beste, en waarom?	Weinig ervaring		
Welke router (in ons assortiment) is naar jouw mening het beste, en waarom?	Weinig ervaring		
Welke firewall (in ons assortiment) is naar jouw mening het beste, en waarom?	Weinig ervaring		
Welke fabrikant levert volgens u de beste support, en waarom?	Cisco, mijn vorige werknemer (KPN) had het hoogste niveau van partnership. Supersnelle responsetijden. (het is niet voor niets heel duur). Ook ervaringen hier zijn goed te noemen voor zover ik weet, ookal zijn wij geen partner		
Welke netwerkapparatuur die wij geleverd hebben vind je ronduit slecht, en waarom? (switch, router, firewall, merk)	Fortigate Firewall/router bij ACA, niet door ons geleverd maar het is een drama apparaat. Ik probeerde de firmware te updaten maar het apparaat gaf geen feedback. Uiteindelijk reboot hij vanzelf zonder melding 5 minuten later. Daarnaast vaak voor deze firewall heen en weer gereden omdat hij er weer eens uit lag. Fortigate is naar mijn mening plastic rotzooi met onduidelijke klungelige interface.		
Wat mis je qua functionaliteiten/performance/etc. aan de huidige gebruikte producten/technologieën	Wij kijken niet vaak genoeg naar de troughput van switches. Waardoor netwerken uiteindelijk traag worden. De goedkopere apparatuur heeft vaak lagere doorvoersnelheid.		
Als er nog dingen zijn die je wil toevoegen dan kan dat in dit hier.(Hier staat ook informatie die buiten de vragen valt)	Ik wil graag dat Constant IT wat meer metaal levert, apparaten van degelijke bouwkwaliteit. Zakelijke apparatuur dient stevig te zijn met een ventilatortje. Eventueel opties om vast te schroeven etc. Minimaal		

	VLAN om mogelijkheden te hebben tot splitsen netwerk Eventueel kunnen we kijken naar Dell, dit zijn vaak rebranded Netgear routers met een "Dell" prijs waar we ook reseller van kunnen worden. Lage prijs, redelijke support met goede prijs kwaliteitverhouding

SERVICE EXECUTION

Vraag	Antwoord		
Naam	Maurits Lagerberg		
Functie:	Team Lead Service Execution		
Welke hardware heb je geconfigureerd na 2012, (switches, firewalls routers?)	Switch	Router	Firewall
	X	X	X
Beschrijf kort je rol binnen Constant IT.			
Met welke hardware fabrikanten heb je ervaring?	Watchguard, Zyxel, Cisco, Linksys HP, modems van diverse providers en Draytek en Apple.		
Welke certificeringen/trainingen op het gebied van netwerkapparatuur heb je?	Geen.		
Hoe schat je je kennis niveau op het gebied van netwerkapparatuur. (op een schaal van 1 t/m 5, waarin 1 geen kennis is en 5 een zeer hoog niveau)	Switch	Routers	Firewalls
	2	2	2
Zou je meer ervaring met netwerkcomponenten willen opdoen? (Zo ja, op welke gebieden)	Nee, ik wil graag management kant op.		
Constant IT heeft veel verschillende hardware van veel verschillende fabrikanten, Welke fabrikant is volgens jou het beste, en waarom?	Watchguard, makkelijk te beheren en in te stellen. Met Draytek zie ik simpel weg te veel fout gaan op de werkvloer. Watchguard lijkt minder storingsgevoelig.		
Welke switch (layer 2) (in ons assortiment) is naar jouw mening het beste, en waarom?	HP Procurves unmanaged		
Welke switch (layer 3) (in ons assortiment) is naar jouw mening het beste, en waarom?	HP Procurve managed.		
Welke router (in ons assortiment) is naar jouw mening het beste, en waarom?	Draytek, omdat we niet veel anders leveren op het moment		
Welke firewall (in ons assortiment) is naar jouw mening het beste, en waarom?	Watchguards die wel al leveren.		
Welke fabrikant levert volgens u de beste support, en waarom?	Niet heel veel ervaring hiermee, Watchguard en Draytek lijken allebei voldoende.		
Welke netwerkapparatuur die wij geleverd hebben vind je ronduit slecht, en waarom? (switch, router, firewall, merk)	Zyxel is echt troep. Ik heb doorgebrande Zyxel routers gezien, software fouten, herconfigureren na een stroomstoring. Dit is het slechtste merk waar ik mee gewerkt heb.		
Wat mis je qua functionaliteiten/performance/etc. aan de huidige gebruikte producten/technologieën	Meldingen van tunnels die down gaan via mail of andere methoden		
Als er nog dingen zijn die je wil toevoegen dan kan dat in dit hier.	Ik kan niet zo 1,2,3 iets bedenken.		

Vraag	Antwoord		
Naam	Niels Kok		
Functie:	Technical Specialist Service Execution		
Welke hardware heb je geconfigureerd na 2012, (switches, firewalls routers?)	Switch	Router	Firewall
	X	X	X
Beschrijf kort je rol binnen Constant IT.	Medewerker SE, tickets op pakken en eerste aanspreekpunt klanten. Support op locatie geven wanneer dit noodzakelijk is.		
Met welke hardware fabrikanten heb je ervaring?	Veel verschillende, binnen Constant IT alleen met Cisco, Watchguard en Draytek.		
Welke certificeringen/trainingen op het gebied van netwerkapparatuur heb je?	Op school, CCNA 1& 2.		
Hoe schat je je kennis niveau op het gebied van netwerkapparatuur. (op een schaal van 1 t/m 5, waarin 1 geen kennis is en 5 een zeer hoog niveau)	Switch	Routers	Firewalls
	3	3	3
Zou je meer ervaring met netwerkcomponenten willen opdoen? (Zo ja, op welke gebieden)	Ik wil/ga CCNA 3 en 4 doen		
Constant IT heeft veel verschillende hardware van veel verschillende fabrikanten, Welke fabrikant is volgens jou het beste, en waarom?	Cisco, werkt straight forward en werkt goed. Wel wat duurder maar dat is het waard.		
Welke switch (layer 2) (in ons assortiment) is naar jouw mening het beste, en waarom?	Sg200 van Cisco, voor de minder rijke klanten		
Welke switch (layer 3) (in ons assortiment) is naar jouw mening het beste, en waarom?	Catalyst 3750, daar hebben we er 2 van geleverd en gestacked. Dit setje was zo rond de 7000 euro. Dit is het beste van het beste maar uiteraard veel te duur voor de normale klant. Ik denk dat we naar Cisco sg200/300/500 moeten kijken.		
Welke router (in ons assortiment) is naar jouw mening het beste, en waarom?	Draytek is het beste voor de minder bedeelde klanten maar deze apparaten zijn alsnog niet goed. Ik kan nog een situatie bedenken met Draytek waarbij er problemen waren. Er waren problemen die niet terug te vinden waren in de logboeken of ergens anders aan terug te leiden waren		
Welke firewall (in ons assortiment) is naar jouw mening het beste, en waarom?	De dure XTM 505 en de goedkopere XTM 22 van Watchguard. Stabiel, weinig offline.		
Welke fabrikant levert volgens u de beste support, en waarom?	HP, Omdat ze carepacks hebben. Carepacks vallen af te sluiten op netwerkapparatuur en servers. Weinig ervaring met Cisco support, want die gaan niet kapot.		
Welke netwerkapparatuur die wij geleverd hebben vind je ronduit slecht, en waarom? (switch, router, firewall, merk)	Draytek AP 800: deed het niet in bepaalde configuraties en gaf maar 2 mbit doorvoer snelheid Draytek 2130: gaat niet goed om met Voip en daar hebben we veel problemen mee gehad. .		
Wat mis je qua functionaliteiten/performance/etc. aan de huidige gebruikte producten/technologieën	Bij de Watchguards niets. Draytek mist wat opties zoals bijvoorbeeld uitgebreide QoS.		
Als er nog dingen zijn die je wil toevoegen dan kan dat in dit hier.	Geen 48 ports switches van een matig merk, 48 port switches zijn sowieso duur dan kun je beter iets meer investeren in een Cisco. Er zitten teveel apparaten aangesloten op een 48 poorts switch om risico te nemen.		

Vraag	Antwoord		
Naam	Kilian Siem		
Functie:	Technical Specialist Service Execution		
Welke hardware heb je geconfigureerd na 2012, (switches, firewalls routers?)	Switch	Router	Firewall
	X	X	
Beschrijf kort je rol binnen Constant IT.	Eerstelijns support die eerstelijns problemen oplost, eventueel op locatie. Betrokken bij projecten die spelen bij klanten en bij interne grote projecten zoals recentelijk het upgraden van Kaseya.		
Met welke hardware fabrikanten heb je ervaring?	Draytek, Cisco en een beetje ervaring met Watchguard		
Welke certificeringen/trainingen op het gebied van netwerkapparatuur heb je?	CCNA 1 en 2.		
Hoe schat je je kennis niveau op het gebied van netwerkapparatuur. (op een schaal van 1 t/m 5, waarin 1 geen kennis is en 5 een zeer hoog niveau)	Switch	Routers	Firewalls
	3	3	2
Zou je meer ervaring met netwerkcomponenten willen opdoen? (Zo ja, op welke gebieden)	Ja, wanneer dit aangeboden wordt. Ik ben niet specifiek op zoek naar netwerktraining. Ik zou me uiteindelijk willen ontwikkelen naar projectmanager.		
Constant IT heeft veel verschillende hardware van veel verschillende fabrikanten, Welke fabrikant is volgens jou het beste, en waarom?	Cisco, hun primairy business is netwerken wat betekend dat ze enorm ervaren zijn en als eerste innoveren. Ze zullen altijd bezig zijn met netwerken in tegenstellingen tot bijvoorbeeld HP die ook servers levert. Daarnaast is Cisco wereldwijd bekend en wordt wereldwijd gerenommeerd. Het is wel wat duur en er is niet echt een instapmodel. Voor een “instap” Cisco router ben je al snel duur uit.		
Welke switch (layer 2) (in ons assortiment) is naar jouw mening het beste, en waarom?	Geen favoriet, niet voldoende hierin verdiept.		
Welke switch (layer 3) (in ons assortiment) is naar jouw mening het beste, en waarom?	Geen favoriet, niet voldoende hierin verdiept.		
Welke router (in ons assortiment) is naar jouw mening het beste, en waarom?	Ik kan niet zeggen welk type het beste is maar qua merk vind ik Cisco het beste Voor klanten met een lager budget voldoen de Drayteks, nadeel van Draytek is dat de geavanceerde features niet altijd goed te bereiken zijn. Draytek is goed voor klanten die alleen de basis willen.		
Welke firewall (in ons assortiment) is naar jouw mening het beste, en waarom?	Weinig ervaring.		
Welke fabrikant levert volgens u de beste support, en waarom?	Ik kan hier geen duidelijke uitspraak over doen, Cisco, Watchguard en HP hebben allemaal mooie support programma’s. Ik heb eigenlijk nog nooit met RMA’s te maken gehad Ik hoor dat Cisco hierin het beste is omdat ze erg flexibel zijn met RMA’s en omwisselen van hardware.		
Welke netwerkapparatuur die wij geleverd hebben vind je ronduit slecht, en waarom? (switch, router, firewall, merk)	Wij hebben wat TP-Links staan, die hebben eigenlijk geen plaats in de organisatie. We hebben ook nog wat Linksys staan (e2500, e3500), deze vindt ik niet fijn werken omdat het configureren moeizaam gaat. Je bent erg gelimiteerd op een Linksys. Hoewel ik moet zeggen dat het qua prijs-kwaliteitverhouding wel goed zit.		
Wat mis je qua functionaliteiten/performance/etc. aan de huidige gebruikte producten/technologieën	We hebben geen command center van waaruit we alle apparaten kunnen beheren. Watchguard heeft dit deels via Watchguard Dimension waarmee logging goed wordt weergegeven. Logging ontbreekt bij vrijwel alle andere apparaten, we hebben nu alleen online/offline status. Helaas worden apparaat fouten, dingen die geblockt worden niet weergegeven, Dit		

	speelt voornamelijk een rol bij de goedkopere apparaten. Logging is een must have en ik vindt dat we naar apparaten toe moeten die dit niet alleen hebben maar ook duidelijk kunnen weergeven.
Als er nog dingen zijn die je wil toevoegen dan kan dat in dit hier.	We leveren nu voornamelijk Draytek en Watchguards, deze zijn degelijk. Ik ben van mening dat wij nooit rotzooi leveren aan klanten.

Vraag	Antwoord		
Naam	Robin Makkus		
Functie:	Technical Specialist Service Execution		
Welke hardware heb je geconfigureerd na 2012, (switches, firewalls routers?)	Switch	Router	Firewall
	X	X	
Beschrijf kort je rol binnen Constant IT.	Eerstelijns tickets oplossen op afstand en op locatie. Ik ben gespecialiseerd in e-mail migraties.		
Met welke hardware fabrikanten heb je ervaring?	Dratek, Cisco. Netgear.		
Welke certificeringen/trainingen op het gebied van netwerkapparatuur heb je?	CCNA 1 & 2		
Hoe schat je je kennis niveau op het gebied van netwerkapparatuur. (op een schaal van 1 t/m 5, waarin 1 geen kennis is en 5 een zeer hoog niveau)	Switch	Routers	Firewalls
	2	2	2
Zou je meer ervaring met netwerkcomponenten willen opdoen? (Zo ja, op welke gebieden)	Ja, later. Eerst Windows server ervaringen opbouwen en later pas de netwerk kant.		
Constant IT heeft veel verschillende hardware van veel verschillende fabrikanten, Welke fabrikant is volgens jou het beste, en waarom?	Draytek voor klanten die klein zijn met weinig functionaliteiten. Voor de rest van de klanten Cisco omdat ik denk dat dit het meest gebruikt wordt door IT professionals.		
Welke switch (layer 2) (in ons assortiment) is naar jouw mening het beste, en waarom?	Netgear GS108 die onder ons bureau staan.		
Welke switch (layer 3) (in ons assortiment) is naar jouw mening het beste, en waarom?	Cisco, maar ik heb hier weinig ervaring mee		
Welke router (in ons assortiment) is naar jouw mening het beste, en waarom?	Draytek, ik kan hier goed mee overweg.		
Welke firewall (in ons assortiment) is naar jouw mening het beste, en waarom?	Ik heb niet voldoende ervaring, maar wij leveren over het algemeen apparaten van degelijke kwaliteit en de Watchguards zullen ook van voldoende kwaliteit zijn.		
Welke fabrikant levert volgens u de beste support, en waarom?	Ik heb geen ervaringen met support van leveranciers, dat is ook meer een SD aangelegenheid.		
Welke netwerkapparatuur die wij geleverd hebben vind je ronduit slecht, en waarom? (switch, router, firewall, merk)	Van hetgeen waar ik ervaring mee heb vind ik niets slecht. Sommige Draytek routers en accespoints hebben mankementen die niet te verklaren zijn.		
Wat mis je qua functionaliteiten/performance/etc. aan de huidige gebruikte producten/technologieën	Ik mis niets specifieks.		
Als er nog dingen zijn die je wil toevoegen dan kan dat in dit hier.	Nee, eigenlijk weet ik niets meer.		

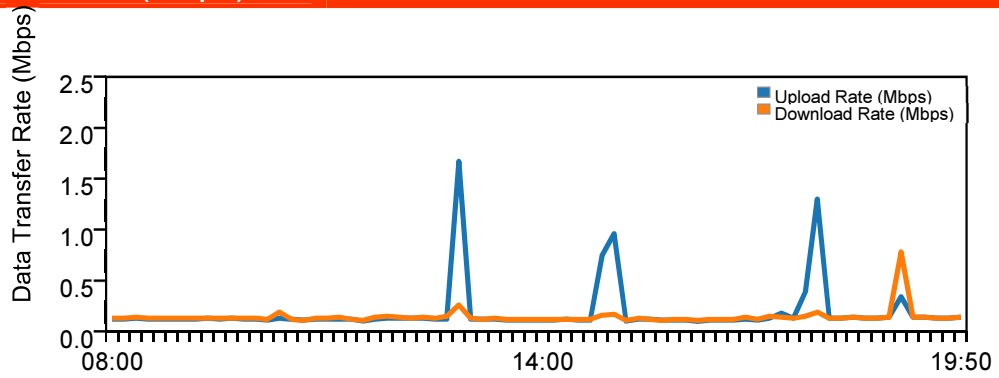
Vraag	Antwoord		
Naam	Thierry Haverkamp		
Functie:	Technical Specialist Service Execution		
Welke hardware heb je geconfigureerd na 2012, (switches, firewalls routers?)	Switch	Router	Firewall
	X	X	
Beschrijf kort je rol binnen Constant IT.	Ik ben Technical specialist, dat houdt in dat ik incidentmeldingen op eerstelijns niveau voor zakelijke klanten moet oplossen en regelen. Voornamelijk goed in het programmeren van routers en switches van Cisco, dat vind ik ook leuk om te doen.		
Met welke hardware fabrikanten heb je ervaring?	Samen met collega's switches geprogrammeerd (Cisco). Netgear en HP, wel geïmplementeerd maar niet geconfigureerd.		
Welke certificeringen/trainingen op het gebied van netwerkapparatuur heb je?	Nog geen certificeren, ik zit nog op school (deeltijd)		
Hoe schat je je kennis niveau op het gebied van netwerkapparatuur. (op een schaal van 1 t/m 5, waarin 1 geen kennis is en 5 een zeer hoog niveau)	Switch	Routers	Firewalls
	3	2	1
Zou je meer ervaring met netwerkcomponenten willen opdoen? (Zo ja, op welke gebieden)	Ja graag, bij Constant IT worden al standaard Windows certificaten aangeboden. Ik wil ook graag de Cisco certificaten behalen zoals sommige andere collega's.		
Constant IT heeft veel verschillende hardware van veel verschillende fabrikanten, Welke fabrikant is volgens jou het beste, en waarom?	Cisco, er is veel leermateriaal beschikbaar. Het inprogrammeren verijst wel wat kennis maar als het eenmaal goed gedaan heb je er geen omkijken meer naar.		
Welke switch (layer 2) (in ons assortiment) is naar jouw mening het beste, en waarom?	De Netgears onder onze tafels. Die leveren wij ook vaak aan klanten.		
Welke switch (layer 3) (in ons assortiment) is naar jouw mening het beste, en waarom?	Catlyst 2960, deze hebben een hoge doorvoer snelheid en zijn (soms) stackable. Daarnaast passen in ze in racks waardoor ze geen schade oplopen. Het voordeel ten opzichte van de kleinere SG modellen is toch wel de uitbreidbaarheid.		
Welke router (in ons assortiment) is naar jouw mening het beste, en waarom?	Drayteck Vigor, eenvoudig in te stellen. Geven niet echt problemen,		
Welke firewall (in ons assortiment) is naar jouw mening het beste, en waarom?	Niet voldoende ervaring, maar de Watchguard lijken goed te voldoen.,		
Welke fabrikant levert volgens u de beste support, en waarom?	HP, als er iets mis is komen ze op de next Business day om apparaten/onderdelen te vervangen. Meestal gaat er niet zoveel kapot.		
Welke netwerkapparatuur die wij geleverd hebben vind je ronduit slecht, en waarom? (switch, router, firewall, merk)	Draytek Vigors zijn qua wi-fi bereik onder de maat. Dit levert soms moeilijke situaties op bij klanten. Dit maakt de apparaten niet slecht maar het is wel vervelend voor zowel de klant als ons.		
Wat mis je qua functionaliteiten/performance/etc. aan de huidige gebruikte producten/technologieën	Ik zou graag zien dat alles 1 gbit poorten heeft, zolang dat ondersteund wordt door de bekabeling bij de klant. Ik denk dat het sowieso tijd is om langzaam aan alle 100Mbit netwerk uit te faseren.		
Als er nog dingen zijn die je wil toevoegen dan kan dat in dit hier.	Nee, ik kan niet snel iets bedenken.		

VPN Bandwidth - Data Transfer Rate

Device(s):	FW-LM-METSU (xx.xx.xxx.xx) 70A60840FEFBC
From:	2014-10-20 08:00:00 (Europe/Berlin)
To:	2014-10-20 20:00:00 (Europe/Berlin)

Data Transfer Rate (Mbps)

)



Time	Upload (MB)	Upload Rate (Mbps)	Download (MB)	Download Rate (Mbps)
2014-10-20 08:00:00	8.99	0.12	9.65	0.13
2014-10-20 08:10:00	8.85	0.12	9.41	0.13
2014-10-20 08:20:00	9.55	0.13	10.23	0.14
2014-10-20 08:30:00	9.24	0.12	9.78	0.13
2014-10-20 08:40:00	8.81	0.12	9.43	0.13
2014-10-20 08:50:00	9.13	0.12	9.76	0.13
2014-10-20 09:00:00	9.06	0.12	9.76	0.13
2014-10-20 09:10:00	8.85	0.12	9.48	0.13

2014-10-20 09:20:00	9.42	0.13	10.04	0.13
2014-10-20 09:30:00	8.74	0.12	9.39	0.13
2014-10-20 09:40:00	9.39	0.13	9.85	0.13
2014-10-20 09:50:00	9.07	0.12	9.66	0.13
2014-10-20 10:00:00	8.71	0.12	9.39	0.13
2014-10-20 10:10:00	8.55	0.11	9.11	0.12
2014-10-20 10:20:00	9.8	0.13	13.92	0.19
2014-10-20 10:30:00	8.74	0.12	9.31	0.12
2014-10-20 10:40:00	8.13	0.11	8.61	0.11
2014-10-20 10:50:00	9.1	0.12	9.74	0.13
2014-10-20 11:00:00	8.83	0.12	9.54	0.13
2014-10-20 11:10:00	8.81	0.12	10.72	0.14

Time	Upload (MB)	Upload Rate (Mbps)	Download (MB)	Download Rate (Mbps)
2014-10-20 11:20:00	8.84	0.12	9.31	0.12
2014-10-20 11:30:00	7.67	0.1	8.22	0.11
2014-10-20 11:40:00	9.24	0.12	10.24	0.14
2014-10-20 11:50:00	10.03	0.13	11.08	0.15
2014-10-20 12:00:00	9.52	0.13	10.27	0.14
2014-10-20 12:10:00	9.48	0.13	10.07	0.13
2014-10-20 12:20:00	9.49	0.13	10.13	0.14
2014-10-20 12:30:00	9.21	0.12	9.92	0.13
2014-10-20 12:40:00	9.2	0.12	11.2	0.15
2014-10-20 12:50:00	125.54	1.67	19.32	0.26
2014-10-20 13:00:00	9.12	0.12	9.84	0.13

2014-10-20 13:10:00	8.78	0.12	9.27	0.12
2014-10-20 13:20:00	9.07	0.12	9.69	0.13
2014-10-20 13:30:00	8.56	0.11	9.18	0.12
2014-10-20 13:40:00	8.41	0.11	9.05	0.12
2014-10-20 13:50:00	8.32	0.11	8.92	0.12
2014-10-20 14:00:00	8.12	0.11	8.79	0.12
2014-10-20 14:10:00	8.29	0.11	8.86	0.12
2014-10-20 14:20:00	8.72	0.12	9.3	0.12
2014-10-20 14:30:00	8.09	0.11	8.75	0.12
2014-10-20 14:40:00	8.35	0.11	8.96	0.12
2014-10-20 14:50:00	55.98	0.75	11.9	0.16
2014-10-20 15:00:00	71.99	0.96	13.1	0.17
2014-10-20 15:10:00	7.47	0.1	8.06	0.11
2014-10-20 15:20:00	9.2	0.12	9.59	0.13
2014-10-20 15:30:00	9.03	0.12	9.3	0.12
2014-10-20 15:40:00	8.14	0.11	8.57	0.11
2014-10-20 15:50:00	8.43	0.11	9.1	0.12
2014-10-20 16:00:00	8.47	0.11	9.19	0.12
2014-10-20 16:10:00	7.66	0.1	8.27	0.11
2014-10-20 16:20:00	8.62	0.11	9.2	0.12
2014-10-20 16:30:00	7.97	0.11	8.68	0.12
2014-10-20 16:40:00	8.33	0.11	8.91	0.12
2014-10-20 16:50:00	8.91	0.12	10.87	0.14
2014-10-20 17:00:00	8.55	0.11	9.23	0.12
2014-10-20 17:10:00	9.72	0.13	11.38	0.15

2014-10-20 17:20:00	13.6	0.18	10.75	0.14
2014-10-20 17:30:00	9.42	0.13	9.7	0.13
2014-10-20 17:40:00	29.57	0.39	10.93	0.15

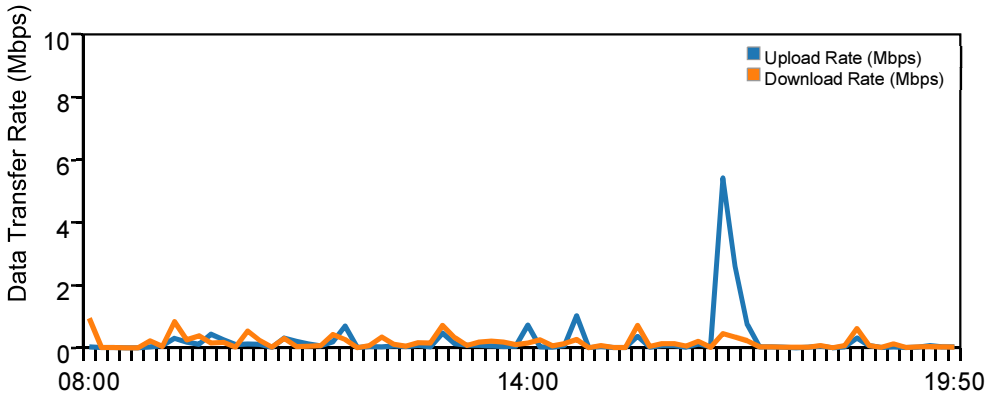
Time	Upload (MB)	Upload Rate (Mbps)	Download (MB)	Download Rate (Mbps)
2014-10-20 17:50:00	97.44	1.3	14.03	0.19
2014-10-20 18:00:00	9.38	0.13	9.39	0.13
2014-10-20 18:10:00	9.44	0.13	9.68	0.13
2014-10-20 18:20:00	10.14	0.14	10.28	0.14
2014-10-20 18:30:00	9.49	0.13	9.68	0.13
2014-10-20 18:40:00	9.71	0.13	9.85	0.13
2014-10-20 18:50:00	10.53	0.14	10.76	0.14
2014-10-20 19:00:00	25.61	0.34	58.28	0.78
2014-10-20 19:10:00	10.54	0.14	10.67	0.14
2014-10-20 19:20:00	10.13	0.14	10.3	0.14
2014-10-20 19:30:00	9.64	0.13	9.73	0.13
2014-10-20 19:40:00	9.72	0.13	9.71	0.13
2014-10-20 19:50:00	10.15	0.14	10.18	0.14
Total: 72	1004.8	0.19	766.42	0.14

FW-LM-RUSTENBURG

VPN Bandwidth - Data Transfer Rate

Device(s):	FW-LM-RUSTENBURG (xx.xx.xx.xx) 70A6083FE4F6B
From:	2014-10-20 08:00:00 (Europe/Berlin)
To:	2014-10-20 20:00:00 (Europe/Berlin)

Data Transfer Rate (Mbps)



Time	Upload (MB)	Upload Rate (Mbps)	Download (MB)	Download Rate (Mbps)
2014-10-20 08:00:00	2.99	0.04	71.59	0.95
2014-10-20 08:10:00	1.14	0.02	1.45	0.02
2014-10-20 08:20:00	1.23	0.02	1.22	0.02
2014-10-20 08:30:00	0.66	0.01	0.83	0.01
2014-10-20 08:40:00	0.88	0.01	0.64	0.01
2014-10-20 08:50:00	2.8	0.04	17.45	0.23
2014-10-20 09:00:00	6.35	0.08	3.73	0.05
2014-10-20 09:10:00	23.29	0.31	63.07	0.84
2014-10-20 09:20:00	14.27	0.19	19.64	0.26
2014-10-20 09:30:00	8.99	0.12	29.02	0.39
2014-10-20 09:40:00	33.16	0.44	11.8	0.16

2014-10-20 09:50:00	20.36	0.27	13.54	0.18
2014-10-20 10:00:00	8.18	0.11	2.44	0.03
2014-10-20 10:10:00	9.47	0.13	40.15	0.54
2014-10-20 10:20:00	9.32	0.12	18.21	0.24
2014-10-20 10:30:00	1.26	0.02	1.92	0.03
2014-10-20 10:40:00	23.96	0.32	23.11	0.31
2014-10-20 10:50:00	15.86	0.21	4.05	0.05
2014-10-20 11:00:00	9.76	0.13	4.7	0.06
2014-10-20 11:10:00	4.97	0.07	5.66	0.08

Time	Upload (MB)	Upload Rate (Mbps)	Download (MB)	Download Rate (Mbps)
2014-10-20 11:20:00	14.91	0.2	32.18	0.43
2014-10-20 11:30:00	52.19	0.7	20.4	0.27
2014-10-20 11:40:00	1.21	0.02	1.01	0.01
2014-10-20 11:50:00	3.46	0.05	5.88	0.08
2014-10-20 12:00:00	2.73	0.04	25.92	0.35
2014-10-20 12:10:00	5.08	0.07	9.08	0.12
2014-10-20 12:20:00	3.83	0.05	4.83	0.06
2014-10-20 12:30:00	6.79	0.09	13.07	0.17
2014-10-20 12:40:00	3.16	0.04	11.8	0.16
2014-10-20 12:50:00	35.76	0.48	53.81	0.72
2014-10-20 13:00:00	10.52	0.14	24.85	0.33
2014-10-20 13:10:00	6.7	0.09	6.13	0.08
2014-10-20 13:20:00	7.05	0.09	14.61	0.19
2014-10-20 13:30:00	4.9	0.07	16.56	0.22

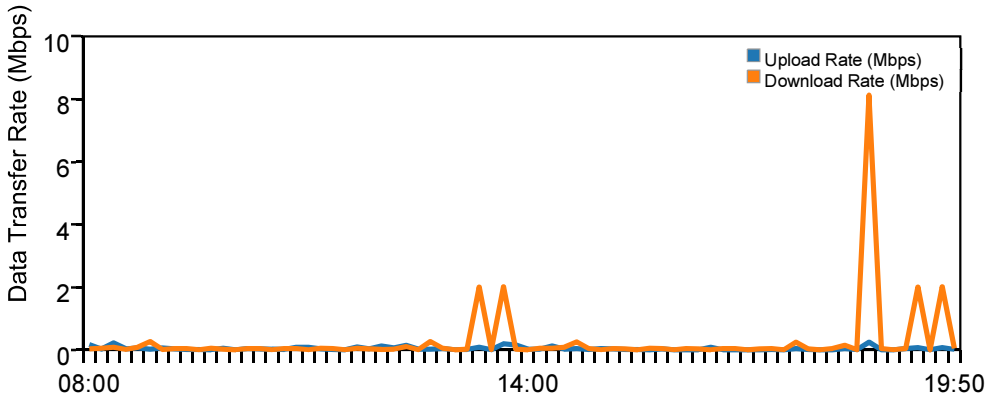
2014-10-20 13:40:00	3.95	0.05	14.31	0.19
2014-10-20 13:50:00	4.24	0.06	7.97	0.11
2014-10-20 14:00:00	55.03	0.73	12.37	0.16
2014-10-20 14:10:00	2.95	0.04	19.63	0.26
2014-10-20 14:20:00	2.19	0.03	4.96	0.07
2014-10-20 14:30:00	5.76	0.08	10.54	0.14
2014-10-20 14:40:00	77.03	1.03	20.14	0.27
2014-10-20 14:50:00	1.11	0.01	1.01	0.01
2014-10-20 15:00:00	3.87	0.05	6.17	0.08
2014-10-20 15:10:00	1.4	0.02	1.7	0.02
2014-10-20 15:20:00	1.49	0.02	1.28	0.02
2014-10-20 15:30:00	27.89	0.37	54.34	0.72
2014-10-20 15:40:00	2.08	0.03	4.09	0.05
2014-10-20 15:50:00	6.33	0.08	10.15	0.14
2014-10-20 16:00:00	5.79	0.08	10.52	0.14
2014-10-20 16:10:00	2.3	0.03	4.53	0.06
2014-10-20 16:20:00	9.39	0.13	15.64	0.21
2014-10-20 16:30:00	2.77	0.04	1.6	0.02
2014-10-20 16:40:00	407.11	5.43	34.48	0.46
2014-10-20 16:50:00	195.86	2.61	26.08	0.35
2014-10-20 17:00:00	56.59	0.75	17.39	0.23
2014-10-20 17:10:00	3.29	0.04	2.76	0.04
2014-10-20 17:20:00	3.17	0.04	2.8	0.04
2014-10-20 17:30:00	1.97	0.03	2.19	0.03
2014-10-20 17:40:00	1.0	0.01	2.45	0.03

Time	Upload (MB)	Upload Rate (Mbps)	Download (MB)	Download Rate (Mbps)
2014-10-20 17:50:00	2.03	0.03	2.25	0.03
2014-10-20 18:00:00	4.5	0.06	6.14	0.08
2014-10-20 18:10:00	1.11	0.01	0.75	0.01
2014-10-20 18:20:00	3.37	0.04	6.31	0.08
2014-10-20 18:30:00	24.3	0.32	46.5	0.62
2014-10-20 18:40:00	6.0	0.08	6.13	0.08
2014-10-20 18:50:00	1.22	0.02	1.65	0.02
2014-10-20 19:00:00	2.8	0.04	10.1	0.13
2014-10-20 19:10:00	1.61	0.02	1.56	0.02
2014-10-20 19:20:00	2.55	0.03	3.09	0.04
2014-10-20 19:30:00	5.75	0.08	3.77	0.05
2014-10-20 19:40:00	3.11	0.04	3.2	0.04
2014-10-20 19:50:00	2.68	0.04	2.32	0.03
Total: 72	1302.78	0.24	957.22	0.18

VPN Bandwidth - Data Transfer Rate

Device(s):	FW-AVC-DC (xx.xx.xx.xx) 80B3063F3E49A
From:	2014-10-20 08:00:00 (Europe/Berlin)
To:	2014-10-20 20:00:00 (Europe/Berlin)

Data Transfer Rate (Mbps)



Time	Upload (MB)	Upload Rate (Mbps)	Download (MB)	Download Rate (Mbps)
2014-10-20 08:00:00	12.76	0.17	2.76	0.04
2014-10-20 08:10:00	2.61	0.03	4.79	0.06
2014-10-20 08:20:00	16.99	0.23	6.52	0.09
2014-10-20 08:30:00	2.7	0.04	1.2	0.02
2014-10-20 08:40:00	5.09	0.07	6.52	0.09
2014-10-20 08:50:00	2.23	0.03	20.33	0.27
2014-10-20 09:00:00	5.11	0.07	1.19	0.02
2014-10-20 09:10:00	3.11	0.04	3.65	0.05
2014-10-20 09:20:00	1.76	0.02	3.68	0.05
2014-10-20 09:30:00	1.37	0.02	1.08	0.01
2014-10-20 09:40:00	1.03	0.01	4.66	0.06

2014-10-20 09:50:00	4.62	0.06	2.58	0.03
2014-10-20 10:00:00	0.81	0.01	0.82	0.01
2014-10-20 10:10:00	3.71	0.05	3.45	0.05
2014-10-20 10:20:00	2.79	0.04	3.8	0.05
2014-10-20 10:30:00	2.2	0.03	0.92	0.01
2014-10-20 10:40:00	1.73	0.02	3.66	0.05
2014-10-20 10:50:00	6.57	0.09	4.02	0.05
2014-10-20 11:00:00	6.98	0.09	1.06	0.01
2014-10-20 11:10:00	2.72	0.04	4.16	0.06

Time	Upload (MB)	Upload Rate (Mbps)	Download (MB)	Download Rate (Mbps)
2014-10-20 11:20:00	1.68	0.02	3.38	0.05
2014-10-20 11:30:00	0.93	0.01	0.85	0.01
2014-10-20 11:40:00	7.5	0.1	4.59	0.06
2014-10-20 11:50:00	3.0	0.04	3.36	0.04
2014-10-20 12:00:00	9.73	0.13	1.75	0.02
2014-10-20 12:10:00	5.16	0.07	2.61	0.03
2014-10-20 12:20:00	10.9	0.15	8.17	0.11
2014-10-20 12:30:00	2.19	0.03	0.83	0.01
2014-10-20 12:40:00	1.97	0.03	20.58	0.27
2014-10-20 12:50:00	3.66	0.05	4.23	0.06
2014-10-20 13:00:00	1.11	0.01	0.85	0.01
2014-10-20 13:10:00	1.8	0.02	2.39	0.03
2014-10-20 13:20:00	6.39	0.09	151.02	2.01
2014-10-20 13:30:00	0.87	0.01	1.19	0.02

2014-10-20 13:40:00	14.79	0.2	151.73	2.02
2014-10-20 13:50:00	11.98	0.16	2.47	0.03
2014-10-20 14:00:00	2.13	0.03	0.88	0.01
2014-10-20 14:10:00	2.38	0.03	4.51	0.06
2014-10-20 14:20:00	10.09	0.13	4.27	0.06
2014-10-20 14:30:00	2.35	0.03	6.48	0.09
2014-10-20 14:40:00	3.73	0.05	19.7	0.26
2014-10-20 14:50:00	1.27	0.02	4.07	0.05
2014-10-20 15:00:00	3.76	0.05	1.07	0.01
2014-10-20 15:10:00	2.97	0.04	3.73	0.05
2014-10-20 15:20:00	1.85	0.02	2.86	0.04
2014-10-20 15:30:00	1.14	0.02	0.82	0.01
2014-10-20 15:40:00	0.91	0.01	4.41	0.06
2014-10-20 15:50:00	3.35	0.04	3.54	0.05
2014-10-20 16:00:00	0.77	0.01	0.83	0.01
2014-10-20 16:10:00	1.1	0.01	3.55	0.05
2014-10-20 16:20:00	0.77	0.01	2.71	0.04
2014-10-20 16:30:00	6.54	0.09	1.06	0.01
2014-10-20 16:40:00	0.8	0.01	4.08	0.05
2014-10-20 16:50:00	0.8	0.01	3.72	0.05
2014-10-20 17:00:00	0.58	0.01	0.85	0.01
2014-10-20 17:10:00	0.94	0.01	2.72	0.04
2014-10-20 17:20:00	1.65	0.02	3.8	0.05
2014-10-20 17:30:00	0.9	0.01	0.89	0.01
2014-10-20 17:40:00	4.11	0.05	18.41	0.25

Time	Upload (MB)	Upload Rate (Mbps)	Download (MB)	Download Rate (Mbps)
2014-10-20 17:50:00	1.69	0.02	3.08	0.04
2014-10-20 18:00:00	0.64	0.01	0.88	0.01
2014-10-20 18:10:00	0.92	0.01	3.66	0.05
2014-10-20 18:20:00	3.55	0.05	10.96	0.15
2014-10-20 18:30:00	0.76	0.01	0.93	0.01
2014-10-20 18:40:00	18.75	0.25	609.74	8.13
2014-10-20 18:50:00	0.77	0.01	3.94	0.05
2014-10-20 19:00:00	0.72	0.01	0.89	0.01
2014-10-20 19:10:00	3.8	0.05	3.61	0.05
2014-10-20 19:20:00	6.14	0.08	151.1	2.01
2014-10-20 19:30:00	0.61	0.01	0.92	0.01
2014-10-20 19:40:00	6.36	0.08	151.31	2.02
2014-10-20 19:50:00	1.29	0.02	3.77	0.05
Total: 72	271.44	0.05	1484.6	0.27

Constant IT

Vergelijkend onderzoek

Constant IT

26 november 2014, Chris de Keijzer
Opleiding: System & Network engineering
Studentnummer: 1591134
Telefoonnummer: 06-10181296
Versie: 1.0

2 DOCUMENTINFORMATIE

Documentbeheer en Goedkeuring

Versie	Auteur	Opmerkingen	Document Eigenaar	Datum
0.1	Chris de Keijzer	Eerste draft	Allard Borgart	3-11-2014
0.2	Chris de Keijzer	Feedback Allard verwerkt, alle hoofdstukken afgetypt en voorzien in de afwerking.	Allard Borgart	17-11-2014
0.3	Chris de Keijzer	Feedback Allard en Bas verwerkt	Allard Borgart	19-11-2014
0.4	Chris de keijzer	Hoofdstuk indeling gewijzigd ten behoeve van leesbaarheid.	Allard Borgart	24-11-2014
1.0	Chris de Keijzer	Afwerking en laatste punten Bas vererkt	Allard Borgart	26-11-2014

Dit document is beoordeeld door

Versie	Naam	Functie	Datum beoordeling
0.1	Allard Borgart	ICT manager	3-11-2014
0.2	Bas de Zeeuw	Technisch specialist	18-11-2014
0.3	Bas de Zeeuw	Technisch specialist	19-11-2014
0.4	Bas de Zeeuw	Technisch specialist	24-11-2014

Dit document is goedgekeurd door

Versie	Naam	Functie	Datum beoordeling
1.0			

INHOUDSOPGAVE

Inhoudsopgave 3
Verklarende woordenlijst 4
1 Inleiding 5
2. Vergelijking 5
3. Longlists 6
3.1 Switches P1 6
3.2 Switches P2 7
3.3 Switches P3 8
3.4 Routers P1 9
3.5 Routers & firewalls P2 10
3.5 Routers & firewalls P3 11
4. Specifieke eisen 12
4.1 Switches P1 12
4.1.1 Shortlist switches P1 13
4.1.2 Conclusie switches P1 14
4.2 Switches P2 14
4.2.1 Shortlist switches P2 16
4.2.2 Conclusie P2 Switches 17
4.3 Switches P3 17
4.3.1 Shortlist switches P3 19
4.3.2 Conclusie P3 Switches 20
4.4 Routers P1 20
4.4.1 Shortlist routers P1 23
4.4.2 Conclusie routers P1 23
4.5 Routers & firewalls P2 24
4.5.1 Shortlist routers & firewalls P2 26
4.5.2 Conclusie routers & firewalls P2 27
4.6 Routers & firewalls P3 27
4.6.1 Shortlist routers& firewalls P3 28
4.6.2 Conclusie routers & firewalls P3 30
5. Conclusie vergelijkend onderzoek 30
Figurenlijst 31
Bronnen 32

VERKLARENDE WOORDENLIJST

ACL	Access Control Lists welke via regels toegang geven of ontzeggen tot bepaalde netwerkbronnen.
All-in-one oplossing	Eén oplossing die voorziet in alle behoefte, binnen het project wordt hiermee een firewall bedoeld die ook dienst kan doen als router.
CLI	Command Line Interface waarmee via tekstinvoer commando's aan apparatuur wordt doorgevoerd.
Dual WAN	Dual WAN apparatuur heft twee ingangen voor WAN verbindingen en kan deze simultaan gebruiken.
High availability	Een oplossing die altijd beschikbaar is doordat er failover en clustering gebruikt wordt.
Java	Software van een derde partij die in sommige gevallen noodzakelijk is om bepaalde scripts op webpagina's te draaien.
LAN	Local Area Network, dit is het eigen interne netwerk
Layer2	Hiermee wordt layer 2 van het OSI model bedoeld. Veel switches werken op deze laag en kennen dus geen IP adressen maar alleen "frames" en switching gebeurd op basis van MAC adres. (Alani, 2014)
Layer3	Layer 3 is de laag waarop routers en logische paden ofwel routing tables hun werk doen. Deze voorzien in routes op IP basis naar andere netwerkapparatuur. (Alani, 2014)
Longlist	Een lijst met producten die voldoen aan de globale requirements.
Managed switch	Een switch die zoals de naam zegt tot in detail in te stellen valt.
Out of the box	Iets dat werkt zonder dat daar iets voor gedaan hoeft te worden.
QoS	Quality of Service gaat om het garanderen van bepaalde services op het netwerk door prioriteiten te stellen. Denk bijvoorbeeld aan VoIP verkeer dat stabiel moet blijven.
Requirements	De eisen, voor di project zijn deze eerder gedefinieerd in het requirements document.
Shortlist	Een lijst met apparaten die aan eisen en wensen voldoen en waar eventueel goede ervaringen mee zijn. Deze voorkeurslijst is gebaseerd op de longlist
Sizing	Deze term houdt in dat apparatuur passend moet zijn bij een klantcategorie. Denk aan voldoende poorten/doorvoersnelheid.
Smart switch	Een smart switch vult het gat tussen unmanaged en managed switches. Het is een semi-managed switch welke eigenschappen heeft van allebei.
Stacking	Het stapelen van apparatuur, door stacking kunnen twee apparaten (of meer) samenwerken als één.
Subscription based licensing	Dit is het verkrijgen van licenties waarvoor jaarlijks of maandelijks betaald dient te worden. Dit komt vaak voor bij apparatuur die vaak geüpdatet dient te worden.
Unmanaged switch	Een switch die uit de box werkt, er valt niets in te stellen en functioneert nadat de stekker is ingeplugd.
VoIP	Het Voice over Internet Protocol is bellen via het netwerk.
VPN	Een Virtual Private Network is een verbinding die via het internet (WAN) naar een andere locatie loopt waarmee het lijkt alsof er in het LAN gewerkt wordt. Deze verbindingen zijn veelal versleuteld.
VRRP + bron	
WAN	Met een Wide Area Network wordt het internet bedoeld.

1 INLEIDING

Dit document bevat het vergelijkende onderzoek dat gebaseerd is op de verdeling van klanten en requirements die opgesteld zijn in het requirements document. Dit document en de resultaten die hier uit voort vloeien zullen leiden tot een testplan en een proof of concept. In hoofdstuk 2 wordt gestart met het uiteenzetten van de vergelijking, de methode waarop de scoring tot stand komt wordt hierin beschreven. Hoofdstuk 3 bevat de longlists die gemaakt zijn aan de hand van de globale eisen die gesteld zijn in het requirements document. Hoofdstuk 4 bevat de shortlists die alle specifieke eisen zoals opgesteld in het requirements document in vergelijkt. Hoofdstuk 5 bevat de conclusie van het vergelijkende onderzoek en geeft de apparaten weer die het best passend zijn in de verschillende klantcategorieën.

2. VERGELIJKING

Longlists
Producten op de longlist moeten voldoen aan alle gestelde globale eisen om door te stromen naar de longlist. De producten die voldoen gaan naar de shortlist.

Shortlist
Aan de hand van de shortlist worden alle door Constant IT gestelde specifieke eisen gecontroleerd aan de hand van de informatie die te vinden valt op de productpagina's van de producten. De eisen zijn gesorteerd via MoSCoW en de in het requirements document gebruikte verdeling.

Beoordelingsmatrix
De beoordelingsmatrix is geïntegreerd met de shortlist, aan elke MoSCoW eis hangt een numerieke waarde, zie figuur 1. Uiteindelijk worden alle eisen waaraan voldaan is opgeteld en komt hier een waarde uit, daarbij wordt de ervaring van Constant IT met dit product in acht genomen en dit levert extra punten op.
Uiteindelijk wordt er een prijskwaliteit verhouding berekend op basis van het puntenaantal. De berekening hiervoor is prijs gedeeld door het aantal punten. Voor de prijs-kwaliteitverhouding is lager beter en deze zal in acht genomen worden bij de conclusie.

Eis	Waarde
Must have	10
Should have	5
Could have	2
Goede ervaring	20

Figuur 44 Waarde van de eisen

3. LONGLISTS

In dit hoofdstuk worden de apparaten op de longlist tegen de globale eisen gehouden om uiteindelijk tot de shortlist te komen. De globale eisen die gebruikt worden zijn gespecificeerd in het eerder gemaakte requirements document. De producten die door gaan de shortlist worden aangegeven met groen.

3.1 SWITCHES P1

Globale requirements Switches P1
Voldoet aan Requirements
R6
R5
R4 PoE variant beschikbaar
R3 Leverbaar binnen 7 dagen
R2 Voldoet aan sizing requirement. (minimaal 16 poorten)
R1 Binnen budget (tot €150)

	Longlist	R1	R2	R3	R4	R5	R6	
1	Cisco SG100D-08	V	X	V	V			X
2	Cisco SG200-08	V	X	V	V			X
3	Cisco Sg100-24	V	V	V	V			V
4	D-Link DGS1008	V	X	V	V			X
5	D-Link WebSmart DGS-1210-28	V	V	X	V			X
6	HP 1910	X	V	V	V			X
7	HP2530	X	X	V	V			X
8	HP V1910-24G	X	V	V	V			X
9	Linksys LGS124	V	V	V	V			V
10	Netgear GS108	V	X	V	V			V
11	Netgear ProSafe JGS524	V	V	V	V			V
12	Zyxel GS1900	V	X	V	X			X

Figuur 45 Switches P1 - Longlist

3.2 SWITCHES P2

Globale requirements Switches P2
Voldoet aan Requirements
R6
R5 Te beheren via web interface
R4 PoE variant beschikbaar
R3 Leverbaar binnen 7 dagen
R2 Voldoet aan sizing requirement. (van 24 tot 48 poorten)
R1 Binnen budget (van €150 tot €500)

	Longlist	R1	R2	R3	R4	R5	R6	
1	Cisco SG200-26	V	V	V	V	V		V
2	Cisco SG200-50	V	V	V	V	V		V
3	Cisco SG300-20	V	X	V	V	V		X
4	Cisco SG300-28	V	V	V	V	V		V
5	Cisco SG500-28	V	V	V	V	V		V
6	D-Link DGS1210-48	V	V	X	V	V		X
7	HP 2530-24	V	V	X	V	V		X
8	Linksys LGS528	X	V	X	V	V		X
9	Netgear GS516T	V	X	V	V	V		X
10	Netgear Prosafe GSM7224	V	V	V	V	V		V
11	Zyxel 1920-48	V	V	X	V	V		X

Figuur 46 Switches P2 - Longlist

3.3 SWITCHES P3

	Globale requirements Switches P3
	Voldoet aan Requirements
R6	Mogelijkheid tot stacking
R5	Te beheren via web interface
R4	PoE variant beschikbaar
R3	Leverbaar binnen 7 dagen
R2	Voldoet aan sizing requirement. (48 poorten)
R1	Binnen budget (vanaf €500)

	Longlist	R1	R2	R3	R4	R5	R6	
1	Cisco SG500-52	V	V	V	V	V	V	V
2	Cisco SG500X-48	V	V	V	V	V	V	V
3	Cisco Catalyst WS-C2960S-24TS-L	V	X	V	V	V	V	V
4	Cisco Catalyst 2960S-48TS-L	V	V	V	V	V	V	V
5	Cisco Catalyst 2960X-48TS-L	V	V	V	V	V	V	V
6	Catalyst 3650-24T	V	X	V	V	V	V	X
7	HP 2530- 48p	V	V	V	V	V	X	X
8	HP 2910al- 48g	V	V	V	V	V	V	V
9	HP 2920- 48g	V	V	V	V	V	V	V
10	HP 3100-48	V	V	V	V	V	X	X
11	HP 5130-48	V	V	X	V	V	V	X
12	Linksys LG552	V	X	V	V	V	X	X
13	Netgear GS752TPSB	V	X	V	V	V	V	X
14	Zyxel XGS3700	V	V	X	V	V	X	X

Figuur 47 Switches P3 - Longlist

3.4 ROUTERS P1

Globale requirements Routers P1
Voldoet aan Requirements
R6
R5 Kan VLAN's onderscheiden
R4 Als goed beoordeeld door externe partij
R3 Leverbaar binnen 7 dagen
R2 Voldoet aan sizing requirement. (tot 15 gebruikers)
R1 Binnen budget (tot €200)

	Longlist	R1	R2	R3	R4	R5	R6	
1	Cisco RV110w	V	V	V	V[7]	V		V
2	Cisco RV320	V	V	V	V[8]	V		V
3	D-Link DSR250N	V	V	V	X	V		X
4	D-Link DSR500N	V	V	X	X	V		X
5	Draytek Vigor 2130	V	V	V	V[9]	V		V
6	Draytek Vigor 2925Vn+	V	V	V	V[10]	V		V
7	Linksys EA6900	V	V	V	V[11]	V		V
8	Linksys WRT1900	X	V	V	V[12]	V		X
9	Netgear R7000	V	V	V	V[13]	X		X
10	Zyxel USG20	V	V	X	X[14]	V		X

Figuur 48 Routers P1 - Longlist

[7] http://www.smallnetbuilder.com/lanwan/lanwan-reviews/31746-cisco-rv180-vpn-router-reviewed?showall=&start=3
[8] http://www.smallnetbuilder.com/lanwan/lanwan-reviews/32317-cisco-rv320-dual-gigabit-wan-vpn-router-reviewed?showall=&start=3
[9] http://www.smallnetbuilder.com/wireless/wireless-reviews/31132-draytek-vigor-2130n-reviewed
[10] De ervaringen van Constant IT met dit product zijn goed, zie ook de interviews. Echter zijn er geen reviews van externe partijen voor dit apparaat te vinden
[11] http://www.trustedreviews.com/linksys-ea6900-ac1900-802-11ac-router-review
[12] http://www.7tutorials.com/reviewing-linksys-wrt1900ac-best-router-worl
[13] http://www.engadget.com/products/netgear/nighthawk/ac1900/smart
[14] http://www.smallnetbuilder.com/lanwan/lanwan-reviews/31488-zyxel-usg20-unified-security-gateway-reviewed?showall=&start=3

3.5 ROUTERS & FIREWALLS P2

Globale requirements Routers P2
Voldoet aan Requirements
R6
R5
R4 Is een all-in one oplossing. (apparaat is zowel router als firewall)
R3 Leverbaar binnen 7 dagen
R2 Voldoet aan sizing requirement. (15 tot 50 gebruikers)
R1 Binnen budget (van €150 tot €700)

	Longlist	R1	R2	R3	R4	R5	R6	
1	Cisco ASA 5505	V	V	V	V			V
2	Cisco RV325	V	V	V	X			X
3	Dell Sonicwall TZ 215	V	X	X	V			X
4	Draytek Vigor 2960	V	V	X	X			X
5	Fortigate 40C	V	V	V	V			V
6	Watchguard fireboxt10	V	X	V	V			X
7	Watchguard XTM25	V	V	V	V			V
8	Watchguard XTM26	V	V	V	V			V
9	Zyxel USG60	V	V	X	V			X
10	Zyxel USG110	V	V	V	V			V

Figuur 49 Routers P2 - Longlist

3.5 ROUTERS & FIREWALLS P3

Globale requirements Routers P3
Voldoet aan Requirements
R6
R5
R4 Is een all-in one oplossing (apparaat is zowel router als firewall)
R3 Leverbaar binnen 7 dagen
R2 Voldoet aan sizing requirement. (van 50 tot 150 gebruikers)
R1 Binnen budget (vanaf €700)

	Longlist	R1	R2	R3	R4	R5	R6	
1	Cisco ASA5505 11port	V	X	V	V			X
2	Cisco ASA 5512-X	V	X	V	V			X
3	Cisco 2901	V	V	V	X			X
5	Dell SonicWALL NSA 220	V	X	V	V			X
6	Sonicwall NSA 2600	V	V	V	V			V
7	Fortigate60C	V	V	X	V			X
8	Fortigate80CM	V	V	V	V			V
9	Netgear UTM150	V	V	X	V			X
10	Watchguard XTM33	V	V	V	V			V
11	Watchguard XTM330	V	V	V	V			V
12	Watchguard XTM515	V	V	V	V			V
13	Watchguard XTM525	V	V	V	V			V
14	Zyxel USG300	V	V	X	V			X

Figuur 50 Routers P3 - Longlist

4. SPECIFIEKE EISEN

In dit hoofdstuk worden de apparaten tegen de specifieke eisen gehouden wat uiteindelijk een apparaat oplevert dat het best passend is. Daarnaast wordt er algemene informatie gegeven over de apparaten en hun onderscheidende eigenschappen.

4.1 SWITCHES P1

Cisco Sg100-24

De Cisco SG100 is een switch die op zo'n manier opgebouwd is dat er geen configuratie en beheer nodig is en het apparaat out of the box werkt. De switch is unmanaged maar heeft wel een aantal geavanceerde features, vooral op het gebied van Quality of Service (QoS) zodat ook VoIP verkeer goed werkt. Er wordt geadverteerd met rotsvaste betrouwbaarheid die verwacht wordt van Cisco samen met een zeer snelle "switching capacity" van 48Gbps. De switch bestaat ook in varianten met 8 en 16 poorten. (Cisco, 2012)

Figuur 51 Cisco SG100

Linksys LGS124

Linksys heeft met deze switch geprobeerd om een snelle en eenvoudige switch oplossing neer te zetten die voldoet aan de verwachtingen van de klanten. De switch is unmanaged en beschikbaar in uitvoeringen met 16 en 24 poorten en omringt in een stevig chassis van metaal. Het apparaat beschikt net als de Cisco switch hierboven over geavanceerde QoS features zodat VoIP verkeer goed werkt. De switch beschikt over 48Gbps aan capaciteit wat betekend dat er niet snel behoefte zal zijn aan vervanging. (Linksys / Belkin international, 2013)

Figuur 52 Linksys LGS124

Netgear ProSafe JGS524

Deze Netgear switch bestaat in versies met 24 poorten en 16 poorten en is qua mogelijkheden hetzelfde als andere twee kandidaten. Ook deze switch heeft 48Gbps aan capaciteit en er zijn QoS features die VoIP goed mogelijk maken. (Netgear, n.d.)

Figuur 53 Netgear ProSafe JGS524

4.1.1 SHORTLIST SWITCHES P1

Globale eisen
Elke switch in deze categorie:

- Kost minder dan 150 euro;
- Beschikt over minimaal 16 poorten;
- Is leverbaar binnen 7 dagen;
- Is ook beschikbaar in een PoE variant.

		Special Requirements Switches P1							
		Producten							
		6							
		5							
		4							
		3 Netgear ProSafe JGS524							
		2 Linksys LGS124							
		1 Cisco Sg100-24							
	Niveau eisen	**Toekomstvastheid**							
1	Must	Ipv6	V	V	V				
2	Must	1 Gbit interfaces	V	V	V				
		Beheerbaarheid							
3	Must	Loggen via webinterface, syslog of mail.	X	X	X				
4	Must	Backup en export van configs	X	X	X				
5	Must	Remote access via telnet, ssh, web, tool.	X	X	X				
		Features							
6	Must	QoS	V	V	V				
7	Must	SNMP	X	X	X				
		Veiligheid							
9	Must	VLANs	V	V	V				
		Ondersteuning							
10	Should	Community	V	V	V				
11	Could	Certificering & partnerships	V	V	X				
		Prijs	€140,01	€100,06	€110,01				
		Prijs per poort	€5,8	€4,1	€5,6				
		Goede ervaringen Constant IT	X	X	X				
		Punten:	47	47	45				
		Prijs-kwaliteitverhouding	2,97	2,12	2,44				

Figuur 54 Switches P1 - Shortlist

*Notities: Eisen 3,4,5 en 7 zijn niet beschikbaar omdat dit alle unmanaged switches betreft.

4.1.2 CONCLUSIE SWITCHES P1

De shortlist wijst uit dat de Linksys LGS 124 het best passende apparaat is op basis van de verzamelde requirements. Echter zal met geen van deze switches een slechte koop gedaan worden gezien ze qua features allemaal erg dichtbij elkaar liggen. Het enige onderscheid is de lage prijs van de Linksys switch wat betekend dat de prijs-kwaliteitverhouding beter is dan die van de anderen.

4.2 SWITCHES P2

Cisco SG200-26

De Cisco SG200's zijn de instap managed switches van Cisco maar eigenlijk is deze switch bedoeld om het gat tussen unmanaged en managed switches op te vullen, deze switch is een zogenoemde smart switch welke features heeft van beiden typen. De switch valt te managen en in te stellen via de webinterface maar kan geen gebruik maken van typische managed functionaliteiten als telnet of SSH. Er wordt gepoogd Cisco kwaliteit te leveren met een scherpe prijs. De switches functioneren alleen op laag 2, er is dus geen mogelijkheid om routering te doen of om ACLs te maken. De vergelijking maakt onderscheid tussen de SG200-26 en de SG200-50, welke inhoudelijk hetzelfde zijn en slechts verschillende poort aantallen hebben. Recente updates van Cisco hebben ervoor gezorgd dat deze switch steeds meer managed wordt en er worden zelfs nu in 2014 nog features toegevoegd. (Cisco, 2013)

Figuur 55 Cisco SG200-50

Cisco SG300-28

De Cisco SG300 is een stap hoger dan de eerder genoemde SG200 qua features en prijs, maar verschilt niet qua hardware bijna niet van de SG200. Het primaire verschil is dat er layer 3 mogelijkheden zijn zoals ACL's en IP routes en dat de SG300 volledig managed is wat betekend dat er ook gebruik gemaakt kan worden van Telnet en SSH. Daarnaast is er ook een vaste console aansluiting aanwezig wat van uit een beheers perspectief zeer wenselijk is. De verschillen tussen de SG300 en SG200 zijn dus softwarematig met uitzondering van de console port. (Cisco, 2013)

Figuur 56 Cisco SG300-28

Cisco SG500-28
De Cisco SG500 is de high end switch van de Cisco SME (small and medium enterprises) switch serie. Met deze switch kunnen geavanceerde zaken als stacking worden uitgevoerd, hoewel dit geen vereiste is binnen de gestelde categorie heeft dit weldegelijk een toegevoegde waarde. Deze switch is zeer geschikt voor bedrijven die het uiterste vragen van hun switch. Deze switch biedt als enige switch binnen in de P2 categorie de mogelijkheid om VTP te gebruiken om VLANs te verspreiden wat het beheer vereenvoudigd. Binnen de vergelijking is vooral de vraag of de hogere prijs wel te rechtvaardigen valt als deze vergeleken wordt met de andere switches in deze categorie. (Cisco, 2013)

Figuur 57 Cisco SG500-28

Netgear Prosafe GSM7224
De Netgear Prosafe is het antwoord van Netgear op de SG300 die qua prijs vrijwel gelijk is, daarnaast zijn de features ook vrijwel gelijk. De Netgear kan net als de SG300 ook layer 3 functionaliteiten gebruiken en is daarmee een interessant alternatief. De Netgear Prosafes worden door de fabrikant aangeprezen als zeer kosteneffectief. (Netgear, 2009)

Figuur 58 Netgear Prosafe GSM7224

4.2.1 SHORTLIST SWITCHES P2

Globale eisen

Elke switch in deze categorie:

- Kost minder dan 500 euro;
- Beschikt over 24-48 poorten;
- Is leverbaar binnen 7 dagen;
- Is ook beschikbaar in een PoE variant;
- Heeft een webinterface.

		Special Requirements Switches P2							
		Producten							
				4 Netgear Prosafe GSM7224					
				3 Cisco SG500-28					
				2 Cisco SG300-28					
				1 Cisco SG200-26/50					
	Niveau eisen	**Toekomstvastheid**							
1	Must	Ipv6	V	V	V	V			
2	Must	Gbit interfaces	V	V	V	V			
3	Should	Mogelijkheden tot failover	V	V	V	V			
4	Could	Stacking	X	X	V	X			
		Beheerbaarheid							
5	Must	Loggen via webinterface, syslog of mail.	V	V	V	V			
6	Must	Backup en export van configs	V	V	V	V			
7	Must	Remote access via telnet, ssh, web, tool.	V	V	V	V			
8	Should	Notificaties (send mail when down)	X	X	X	X			
9	Should	Reporting op basis van vooraf ingestelde paramaters	X	X	X	X			
10	Should	Console Port	X	V	V	V			
11	Should	Diagnostische tools	V	V	V	V			
12	Could	Opties voor centraal beheer	X	X	X	X			
		Features							
13	Must	Etherchannel(LACP)	V	V	V	V			
14	Must	QoS	V	V	V	V			
15	Must	LLDP	V	V	V	V			
16	Must	SNMP	X	V	V	V			
17	Should	Layer 3 functionaliteit	X	V	V	V			
		Veiligheid							
18	Must	VLAN	V	V	V	V			
19	Should	VLAN verspreiding	X	X	V	X			
20	Should	Security levels instellen	X	V	V	X			
21	Should	ACL	X	V	V	V			
		Ondersteuning							
22	Must	Community	V	V	V	V			
23	Must	Helpdesk support	V	V	V	V			
24	Should	Certificering & partnerships	V	V	V	V			
25	Could	Training	V	V	V	V			
		Prijs	€208	€372	€478	€319			
		Prijs per poort	€8	€13	€17	€13			
		Goede ervaringen Constant IT (+20 punten)	V	V	V	X			
		Punten:	132+20	167+20	175+20	165			
		Prijs-kwaliteitverhouding	1,37	2,04	2,45	1,96			

Figuur 59 Switches P2 - Shortlist

4.2.2 CONCLUSIE P2 SWITCHES

De shortlist wijst uit dat alle producten die getest zijn aan de “must have” eisen voldoen. De SG200 is commercieel gezien het meest ideaal. Deze biedt voldoende features voor een zeer sterke prijs. Echter is de aanbeveling voor deze categorie de SG300 omdat deze meer compleet is qua features. De SG300 voldoet aan bijna alle door Constant IT gestelde eisen. De SG500 is meer dan 100 euro duurder en biedt qua features niet veel meer dan de SG300. De Netgear GSM 7224 scoort gelijk met de SG300 qua features maar de SG300 heeft meer poorten waardoor de prijs per poort gelijk blijft. Echter heeft men goede ervaringen met de SG300 en is er dus geen reden om in deze categorie een ander product aan te bevelen.

4.3 SWITCHES P3

Cisco SG500-52 / Cisco SG500X-48

De SG500 is zoals eerder gezegd de high end Small and Medium Enterprise (SME) switch van Cisco, de SG500 doet in deze categorie mee als prijsvechter en is de goedkoopste switch in deze categorie. De vergelijking gaat uitwijzen of de hogere prijzen van de andere switches te rechtvaardigen zijn.
De SG500X is bijna hetzelfde als de SG500 maar het verschil is dat de SG500X de mogelijkheid heeft om 10GE aansluitingen te gebruiken voor stacking. Daarnaast heeft de SG500X de mogelijkheid het VRRP (Virtual Router Redundancy Protocol) te gebruiken wat de mogelijkheid geeft om meerdere stacks van deze switch in failover te laten draaien.
(Cisco, 2013)

Figuur 60 SG500 /SG500X

Cisco Catalyst 2960S-48TS-L / Cisco Catalyst 2960X-48TS-L

Dit zijn de instap “enterprise” switches van Cisco, het belangrijkste verschil met de SME switches zoals de SG500 is dat deze Cisco IOS als besturingssysteem draaien. Dit betekend dat er voornamelijk via de command line gewerkt moet worden maar dat wel alles tot detail is in te stellen. Echter valt er wel een webinterface aan te zetten via de command line waarmee basis configuratie gedaan kan worden. Daarnaast heet Cisco een ook een grafisch tool waarmee alles geconfigureerd kan worden, deze heet Cisco network assistent (Cisco, 2013)
In de vergelijking wordt er onderscheid gemaakt tussen de Catalyst 2960S en X. De grootste verschillen tussen deze twee typen zijn dat de X versie tweemaal zoveel snelheid heeft en dat er van de X een stack van 8 switches gemaakt kan worden. De S versie kan maximaal met 4 switches gestacked worden. (Cisco, 2013)

Figuur 61 Cisco Catalyst 2960S-48TS-L

HP 2910al- 48g

HP probeert met de 2910al een switch neer te zetten die overal in een enterprise past. Dit betekend dat de switch ingezet kan worden om gebruikers van connectiviteit te voorzien alsmede een betrouwbare oplossing te geven voor de “core” van get netwerk dat snelheid en redundant uitgevoerd moet zijn. Deze switch probeert de meest kosten effectieve oplossing te zijn in zijn klasse. De HP switches in deze categorie draaien op zowel een CLI interface als een webinterface. De webinterface is echter op Java gebaseerd wat betekend dat er applicaties van derde partijen aan te pas moeten komen.

Figuur 62 HP 2910al-48 voor- en achterzijde

HP 2920- 48g

Deze HP switch is een maat groter dan de HP2910al en er zijn wat extra mogelijkheden voor backups en management. Zo zijn er bijvoorbeeld een twee OS images aanwezig en is het eenvoudig om fouten met het apparaat te achterhalen via het OS. De switch werkt op hetzelfde OS als de 2910al en heeft dus ook dezelfde Java software nodig om beheerd te worden. Daarnaast heeft deze switch oneindig recht op downloads van HP (zolang deze gemaakt worden) en er is een “lifetime warranty” die voorziet in next business day delivery bij problemen. (HP, 2013)

Figuur 63 HP2920-48g

4.3.1 SHORTLIST SWITCHES P3

Globale eisen

Elke switch in deze categorie:

- Kost minder dan 150 euro;
- Beschikt over minimaal 16 poorten;
- Is leverbaar binnen 7 dagen;
- Is ook beschikbaar in een PoE variant;
- Heeft een webinterface;
- Kan gestackt worden.

		Special Requirements Switches P3							
		Producten							
		6 HP 2920- 48g							
		5 HP 2910al- 48g							
		Cisco Catalyst 2960X-48TS-L							
		Cisco Catalyst 2960S-48TS-L							
		Cisco SG500X-48							
		1 Cisco SG500-52							
	Niveau eisen	**Toekomstvastheid**							
1	Must	Ipv6	V	V	V	V	V	V	
2	Must	Gbit interfaces	V	V	V	V	V	V	
3	Should	Uitbreidbaarheid (extra poorten)	V	V	V	V	V	V	
4	Should	Mogelijkheden tot failover	V	V	V	V	V	V	
5	Could	Support voor 10GE via koper of fiber	X	V	V	V	V	V	
6	Must	Stacking	V	V	V	V	V	V	
		Beheerbaarheid							
7	Must	Loggen via webinterface, syslog of mail.	V	V	V	V	V	V	
8	Must	Backup en export van configs	V	V	V	V	V	V	
9	Must	Remote access via telnet, ssh, web, tool.	V	V	V	V	V	V	
10	Should	Notificaties (send mail when down)	X	X	X	X	X	X	
12	Should	Console Port	V	V	V	V	V	V	
13	Should	Reporting op basis van vooraf ingestelde paramaters	X	X	V**	V**	X	X	
14	Should	Diagnostische tools	V	V	V	V	V	V	
15	Could	Opties voor centraal beheer	V*	V*	V*	V*	V*	V*	
		Features							
16	Must	Etherchannel(LACP)	V	V	V	V	V	V	
17	Must	QoS	V	V	V	V	V	V	
18	Must	LLDP	V	V	V	V	V	V	
19	Must	SNMP	V	V	V	V	V	V	
20	Should	Layer 3 functionaliteit	V	V	V	V	V	V	
		Veiligheid							
21	Must	VLAN	V	V	V	V	V	V	
22	Must	VLAN verspreiding	V	V	V	V	V	V	
23	Should	Security levels instellen	V	V	V	V	V	V	
24	Should	ACL	V	V	V	V	V	V	
		Ondersteuning							
25	Must	Community	V	V	V	V	V	V	
26	Must	Helpdesk support	V	V	V	V	V	V	
27	Should	Certificering & partnerships	V	V	V	V	V	V	
28	Could	Training	V	V	V	V	V	V	
		Prijs	€775	€1115	€1880	€2078	€2117	€1799	
		Prijs per poort	€15	€23	€39	€43	€44	€37	
		Goede ervaringen Constant IT	V	V	V	V	X	X	
		Punten:	184+20	186+20	191+20	191+20	186	186	
		Prijs-kwaliteitverhouding	3,45	5.41	8,90	10.33	12,02	10,22	

Figuur 64 Switches P3 - Shortlist

** Een stack van switches kan beheerd worden op één IP, niet alle switches over alle klanten.

*** Via Cisco IOS Flexible NetFlow (Cisco, 2008).

4.3.2 CONCLUSIE P3 SWITCHES

SG500

De SG500 is de high end switch van de Cisco Small and Medium enterprises (SME) serie. De SG500 komt als meest geschikt uit de vergelijking vanwege de prijs-kwaliteitverhouding. De SG500 doet alles wat Constant IT nodig heeft maar mist wel bepaalde features ten opzichte van de anderen. Zo is er bijvoorbeeld geen 10GE module om mee te stacken en ook geen VRRP protocol aanwezig waarmee meerdere stacks aangemaakt kunnen worden. Echter zijn dit geen must have eisen binnen Constant IT en zijn er geen klanten die hiervan gebruik maken. Dit betekend dat de SG500 aan de eisen voldoet tegen de beste prijs, andere switches zijn vaak tweemaal duurder.

4.4 ROUTERS P1

Cisco RV110w

De Cisco RV110W is de instap router van Cisco met het oog op de zakelijke markt. De router is gericht op de kleinste zakelijke klant en kan maximaal 1 site to site VPN tunnel aan. De router onderscheidt zich vooral door de scherpe prijs en de uitgebreide feature set. De router beschikt ook over Wi-Fi wat betekend dat met dit ene apparaat ene heel bedrijf van alle basisfunctionaliteiten voorzien kan worden.
(Cisco, 2012)

Figuur 65 Cisco RV110w

Cisco RV320
De Cisco RV320 is een router die een stuk geavanceerder is dan de eerder genoemde RV110, de router ondersteund zaken als redundantie via de multi WAN verbinding en kan tot 25 site-to-site VPN tunnels aan. Daarnaast kan er ook een failover via 3G of 4G gebruikt worden via de USB poorten en is er basis verdediging tegen DDOS aanvallen.
Deze router is het zwaargewicht van de instap modellen en is behoorlijk prijzig te noemen binnen deze categorie maar heeft geen wireless mogelijkheden. (Cisco, 2013)

Figuur 66 Cisco RV320

Draytek Vigor 2130
Deze Draytek router onderscheidt zich van de rest van de routers in de markt omdat er gigabit WAN en LAN poorten op het apparaat aanwezig zijn voor een zeer scherpe prijs. Daarnaast is er een mogelijkheid om VPN verbindingen te maken, echter zijn er maar maximaal 2 gelijktijdige VPN verbindingen mogelijk. Qua features doet de router niet veel onder voor de Cisco RV320, wat opvallend is gezien de prijs. (Draytek, n.d.)

Figuur 67 Draytek Vigor 2130

Draytek Vigor 2925Vn+
De Draytek 2925+ is een zeer complete router die tot wel 50VPN tunnels aan kan, hierdoor is de directe vergelijking met de Cisco RV320 snel gelegd. Echter ligt de prijs van deze router zeer hoog maar krijgt men voor deze prijs een zeer compleet apparaat met dual-wan en wireless functionaliteit. Deze router kan ook verbinding maken met het active directory van Microsoft om gebruikers in te laten loggen via radius. Daarnaast kunnen gebruikers eenvoudig beheerd worden via de user management console. Deze router onderscheidt zich omdat er zeer veel beheer mogelijkheden zijn. (Draytek, n.d.)

Figuur 68 Draytek 2925Vn+

Linksys EA6900
De Linksys router is een router die voornamelijk gericht is op particuliere gebruikers en niet op zakelijk gebruikers, echter zijn er wel een aantal zakelijke features aanwezig en onderscheid de router zich door de draadloos snelheden die tot wel 1300Mbps op kunnen lopen. Echter zit een stevig prijskaartje aan deze router en is het nog maar de vraag of deze router wel kan voorzien in de behoeften. (Linksys, n.d.)

Figuur 69 Linksys EA6900

4.4.1 SHORTLIST ROUTERS P1

Globale eisen

Elke router in deze categorie:

- Kost minder dan 500 euro;
- Kan tot 15 gebruikers aan;
- Is leverbaar binnen 7 dagen;
- Is ook beschikbaar in een PoE variant;
- Heeft een webinterface.

Special Requirements –Routers P1
Producten
6
5 Linksys EA6900
4 Draytek Vigor 2925Vn+
3 Draytek Vigor 2130
2 Cisco RV320
1 Cisco RV110w

	Niveau eisen								
		Toekomstvastheid							
1	Must	Gigabit poorten	X	V	V	V	V		
2	Must	IPv6	V	V	V	V	V		
3	Could	Uitbreidbaarheid via licenties	X	X	X	X	X		
		Beheerbaarheid							
4	Must	Loggen via webinterface, syslog of mail.	V	V	V	V	V		
5	Should	Diagnostische tools	V	V	V	V	V		
		Features							
6	Must	Site to site VPN	V	V	V	V	X		
7	Must	Voldoende VPN troughput	V	V	V	V	X		
8	Must	VPN failover	X	V	X	V	X		
9	Must	Qos & Traffic management/shaping	V	V	V	V	V		
10	Must	DHCP	V	V	V	V	V		
11	Must	SNMP	V	V	V	V	X		
12	Must	Verschillende NAT types (specifiek NAT loopback)	X	X	X	X	X		
13	Should	Modem functionaliteit	X	X	X	X	X		
		Veiligheid							
14	Must	VLAN support	V	V	V	V	V		
		Ondersteuning							
15	Must	Community	V	V	V	V	X		
16	Should	Certificering & partnerships	V	V	V	V	X		
		Prijs	€534,2	€174,79	€84	€194	€160		
		Goede ervaringen Constant IT	X	X	V	V	X		
		Punten:	100	120	110 +20	120 +20	70		
		Prijs-kwaliteitverhouding	0,53	1,45	0,64	1,38	2,28		

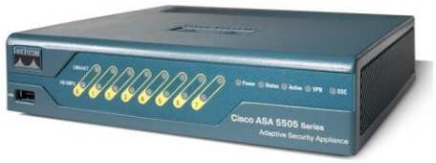
Figuur 70 Routers P1 - Shortlist

4.4.2 CONCLUSIE ROUTERS P1

Het best passende product voor deze categorie is de Draytek Vigor 2130 welke voor een prijs onder de 100 euro bijna net zoveel features kent als de meer dan tweemaal duurdere Draytek Vigor 2925vn+en Cisco RV320. De Cisco RV110w heeft veruit de beste prijs-kwaliteit verhouding maar deze heeft geen gigabit aansluitingen wat toch een gemis is. De Linksys EA6900 laat het op alle fronten afweten tegenover de concurrentie. De Draytek Vigor 2130 is niet de snelste router, maar zal zeker volstaan in P1 omgevingen.

4.5 ROUTERS & FIREWALLS P2

Cisco ASA 5505 (met security+)
De ASA5505 is de instap firewall van Cisco en bevat interessant genoeg dezelfde features als duurdere modellen. Echter zijn er maar 25 VPN sessies tegelijk mogelijk en doen ze veel met licenties. Zo zijn er extra licenties voor Anyconnect VPN gebruikers en zijn er voor bepaalde features zoals high availability een security plus license nodig. Een belangrijk punt van de ASA is dat deze alleen te configureren is via de command line interface wat betekend dat configureren lastig kan zijn. (Cisco, 2014)



Figuur 71 Cisco ASA5505

Fortigate 40C
De Foritigate firewalls zijn kleine all-in-one beveiligingsapparaten die via een webinterface beheerd worden. De 40C is gericht op kleine bedrijven of “branch offices”. Het doel van Fortigate is om de hoeveelheid apparaten terug te dringen door complete apparaten aan te leveren met veel features. Naast alle features is een optionele service die alle definities van onder andere de IPS/IDS automatisch update tegen nieuwe bedreigingen, dit is uiteraard tegen een meerprijs. (Fortinet, 2013)

Figuur 72 Fortigate 40C

Watchguard XTM26
Watchguard levert met de XTM26 een all-in-one oplossing met een scherpe prijs. Het licentiemodel van Watchguard is dat er een basis apparaat gekocht wordt wat vervolgens uitgebreid kan worden met allerlei features zoals IPS, data loss prevention en APT blocker welke zegenoemde “zero day” malware kan stoppen. (Watchguard, 2014). De Watchguard systemen kunnen gebruik maken van Watchguard Dimension, dit is in principe een syslog server maar er wordt ook grafisch weergegeven wat er op het apparaat gebeurd. Er kunnen in principe een oneindige hoeveelheid Watchguards aangesloten woorden op Dimension waardoor het een krachtige tool is om alle Watchguards in de organisatie in het oog te houden(Watchguard, 2014)

Figuur 73 Watchguard XTM26

Zyxel USG110
De Zyxel USG110 is een firewall die gespecialiseerd is in het verlenen van hoge VPN doorvoersnelheden. Deze worden bereikt door de firewall te voorzien van een quad-core CPU en 1GB aan werkgeheugen. De USG110 kan tot 100 VPN verbindingen aan. De USG110 is gepositioneerd als een eenvoudig te beheren firewall die zie specialiseert in VPN doorvoersnelheid, de vergelijking gaat uitwijzen of er niet beknibbeld is op andere features.
(Zyxel, 2014)

Figuur 74 Zyxel USG110

4.5.1 SHORTLIST ROUTERS & FIREWALLS P2

Globale eisen

Elke router en firewall in deze categorie:

- Kost minder dan 700 euro;
- Kan tot 50 gebruikers aan;
- Is leverbaar binnen 7 dagen;
- Is ook beschikbaar in een PoE variant;
- Heeft een webinterface.

Special Requirements –Routers P2
Producten
6
5
4 Zyxel USG110
3 Watchguard XTM26
2 Fortigate 40C
1 Cisco ASA 5505

	Niveau eisen					
		Toekomstvastheid				
1	Must	Multi wan (failover of bundelen)	V	V	V	V
2	Must	Gigabit poorten	X	V	V	V
3	Must	IPv6	V	V	V	V
4	Must	Link aggregation	V	V	V	V
5	Could	Uitbreidbaarheid via licenties	V	V	V	V
		Beheerbaarheid				
6	Must	Loggen via webinterface, syslog of mail.	V	V	V	V
7	Should	Reporting op basis van vooraf ingestelde paramaters	V*	X	V	X
8	Should	Console port aansluiting	V	V	V	V
9	Should	Diagnotische tools	V	X	X	V
		Features				
10	Must	Site to site VPN	V	V	V	V
11	Must	Voldoende VPN troughput	V	V	V	V
12	Must	VPN failover	V	X	V	V
13	Must	Qos & Traffic management/shaping	V	V	V	V
14	Must	DHCP	V	V	V	V
15	Must	SNMP	V	V	V	V
16	Must	Verschillende NAT types (specifiek NAT loopback)	V	X	V	V
17	Should	LDAP/AD integratie	V	V	V	V
18	Should	Modem functionaliteit	X	X	X	X
		Veiligheid				
19	Must	IPsec	V	V	V	V
20	Must	VLAN support	V	V	V	V
21	Must	ACL's	V	V	V	V
22	Should	DDOS herkenning.	X	X	V	X
23	Could	IDS/IPS	V*	V	V	V
24	Could	Security levels instellen	V	V	V	V
25	Could	Audit logs	V	V	V	X
		Ondersteuning				
26	Must	Community	V	X	V	X
27	Must	Helpdesk support	V	V	V	V
28	Should	Certificering & partnerships	V	V	V	V
29	Could	Training	V	V	V	V
		Prijs	€595	€500	€500	€486
		Goede ervaringen Constant IT			V	
		Punten:	203	167	205+20	188
		Prijs-kwaliteitverhouding	2,93	2,99	1,77	2,58

Figuur 75 Routers P2 - Shortlist

*Via Netflow, dit externe pakket is een extra investering.

4.5.2 CONCLUSIE ROUTERS & FIREWALLS P2

Het beste apparaat in de P2 categorie is de Watchguard XTM26, deze voldoet aan bijna alle requirements die gesteld zijn door Constant IT en doet dat tegen een goede prijs. De Cisco ASA 5505 heeft ook zeer veel goede features aan boort maar mist vervolgens 1Gbit poorten, wat voor een apparaat met een prijs van bijna 600 euro toch wat vreemd is. De andere opties voldoen niet aan de gestelde requirements en scoren te laag qua punten.

4.6 ROUTERS & FIREWALLS P3

Sonicwall NSA 2600

De Network Security Appliance(NSA) serie van Dell richt zich op het laten samen komen van beveiliging en performance. Dit betekend dat de firewalls met multi-core processoren zijn uitgerust en dat er zeer veel features beschikbaar zijn. Volgens de Sonicwall website is de NSA2600 een all-in-one device dat eenvoudig te beheren valt door het “Global Management System” welke honderden of zelfs duizenden Sonicwalls vanaf één management console kan beheren. (Dell, 2013)

Figuur 76 Sonicwall NSA 2600

Fortigate80CM

De 80CM is gericht op middelgrote bedrijven binnen een enterprise en heeft als kan alle andere apparaten binnen een bedrijf overbodig te maken. De reden hiervoor is dat de 80CM wireless netwerken kan opzetten maar ook een modempoort heeft wat een sterk onderscheidt vormt met de andere firewalls in deze categorie. Daarnaast kunnen er met Fortimanager en Fortianalyser duizenden Fortigate firewalls beheerd worden. De Fortigates hebben net als Watchguard allerlei “subscription based services” zoals webfiltering, antispam en intrusion prevention. (Fortinet, 2013)

Figuur 77 Fortigate 80CM voor- en achter

Watchguard XTM330 en 33
De XTM 3 serie is de grotere broer van de eerder genoemde XTM2 serie en bestaat uit twee modellen.
Enerzijds is er de XTM33 wat een klein apparaat is dat geschikt is voor het aansluiten van kleine bedrijven en anderzijds is er de grote XTM330 welke een rackmounted apparaat is. Qua features verschillen de apparaten inhoudelijk niet, de enige verschillen zijn fysiek, zo is de XTM330 met snellere hardware uitgerust en is deze niet passief gekoeld. De XTM330 is geschikt voor plaatsing in datacentra of hoofdkantoren terwijl de XTM33 de verschillende “branch offices” moet koppelen aan de infrastructuur. (Watchguard, 2014)

Figuur 79 Watchguard XTM 33


Figuur 78 Watchguard XTM330

Watchguard XTM515/525
De XTM 5 serie zijn snellere versies van de XTM330, de XTM515 welke het instapmodel is van de XTM 5 serie is ongeveer 30% sneller dan de XTM 330. Opvolgende versies zetten deze lijn voort en hebben telkens ongeveer 30% meer capaciteit. (Watchguard, 2014)


Figuur 80 Watchguard XTM 525

4.6.1 SHORTLIST ROUTERS& FIREWALLS P3
Globale eisen
Elke router en firewall in deze categorie:

- Kost meer dan 700 euro;
- Kan tot 100 gebruikers aan;
- Is leverbaar binnen 7 dagen;
- Is ook beschikbaar in een PoE variant;
- Is een all-in-one oplossing.

		Special Requirements –Routers P3						
		Producten						
		6						
		5 Watchguard XTM5XX (515/525)						
		4 Watchguard XTM330						
		3 Watchguard XTM33						
		2 Fortigate80CM						
		1 Sonicwall NSA 2600						
	Niveau eisen							
		Toekomstvastheid						
1	Must	Mogelijkheid tot clustering	V	V	V	V	V	
2	Must	Multi wan (failover of bundelen)	V	V	V	V	V	
3	Must	Gigabit poorten	V	V	V	V	V	
4	Must	IPv6	V	V	V	V	V	
5	Must	Link aggregation	V	V	V	V	V	
6	Could	Uitbreidbaarheid via licenties	X	V	V	V	V	
		Beheerbaarheid						
7	Must	Loggen via webinterface, syslog of mail.	V	V	V	V	V	
8	Should	Reporting op basis van vooraf ingestelde paramaters	V*	V	V	V	V	
9	Should	Console port aansluiting	V	V	X	V	V	
10	Should	Diagnotische tools	V	X	V	V	V	
11	Could	Opties voor centraal beheer	V	V	V	V	V	
		Features						
12	Must	Site to site VPN	V	V	V	V	V	
13	Must	Voldoende VPN troughput	V	V	V	V	V	
14	Must	VPN failover	V	V	V	V	V	
15	Must	Qos & Traffic management/shaping	V	V	V	V	V	
16	Must	Policy based traffic management (ACL)	V	V	V	V	V	
17	Must	DHCP	V	V	V	V	V	
18	Must	SNMP	V	V	V	V	V	
19	Must	Verschillende NAT types (specifiek NAT loopback)	V	X	V	V	V	
20	Should	LDAP/AD integratie	V	V	V	V	V	
21	Should	Modem functionaliteit	X	V	X	X	X	
		Veiligheid						
22	Must	IPsec	V	V	V	V	V	
23	Must	VLAN support	V	V	V	V	V	
24	Must	ACL's	V	V	V	V	V	
25	Should	Proxy support / Web filtering.	V	V	V	V	V	
26	Should	DDOS herkenning.	V	V	V	V	V	
27	Could	IDS/IPS	V	V	V	V	V	
28	Could	Security levels instellen	V	X	V	V	V	
29	Could	Audit logs	V	V	V	V	V	
		Ondersteuning						
30	Must	Community	X	V	V	V	V	
31	Must	Helpdesk support	V	V	V	V	V	
32	Should	Certificering & partnerships	V	V	V	V	V	
33	Could	Training	V	V	V	V	V	
		Prijs	€1810	€1200	€1100	€1400	€2034	
		Goede ervaringen Constant IT			V	V		
		Punten:	225	238	237 +20	239+20	239	
		Prijs-kwaliteitverhouding	8,04	5,04	4,28	5,40	8,51	

Figuur 81 Routers P3 - Shortlist

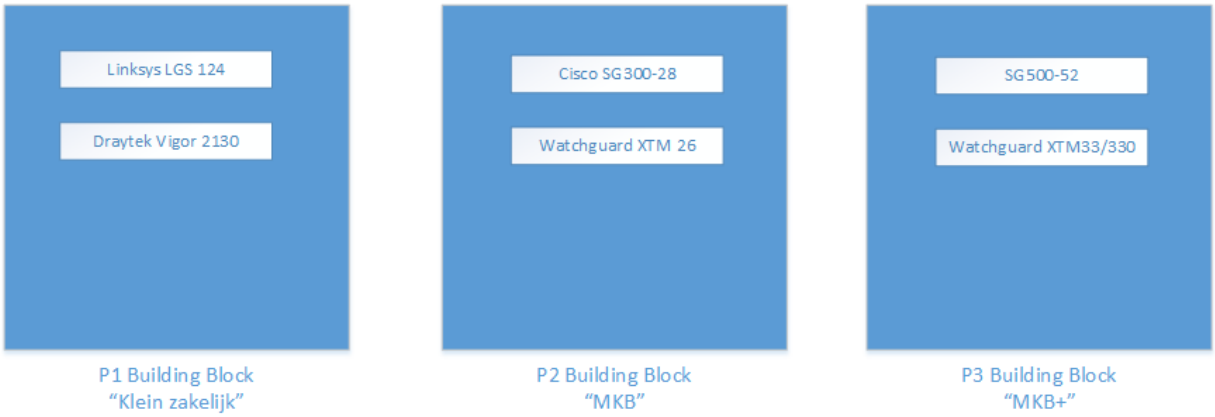
* Via Netflow, dit externe pakket is een extra investering.

4.6.2 CONCLUSIE ROUTERS & FIREWALLS P3

In deze categorie liggen alle apparaten erg dicht bij elkaar qua resultaten met uitzondering van de SonicWall 2600. Echter omdat men al ervaring heeft met de Watchguards en deze al vaak ingezet worden is het geen goed idee om hier van af te stappen omdat andere apparaten niet veel meer bieden. Daarnaast hebben de Watchguard een goede prijs kwaliteitverhouding.

5. CONCLUSIE VERGELIJKEND ONDERZOEK

Het onderzoek heeft geresulteerd in een aantal aanbevolen apparaten welke in de latere hoofstukken in building block vorm aangeleverd worden, het kenmerk van building blocks is dat deze inwisselbaar zijn. De Visio tekening hieronder heeft een onderscheid gemaakt tussen de P1, P2 en P3 categorieën. Echter is het vanzelfsprekend ook mogelijk om een switch van P2 aan een router in P1 te koppelen. Dit betekend dus dat deze zes producten enorm flexibel ingezet kunnen worden. Hieronder een weergave van de best passende producten per categorie.



Figuur 82 Resultaten onderzoek in concept building block vorm

FIGURENLIJST

Figuur 1 Waarde van de eisen 5
Figuur 2 Switches P1 - Longlist 6
Figuur 3 Switches P2 - Longlist 7
Figuur 4 Switches P3 - Longlist 8
Figuur 5 Routers P1 - Longlist 9
Figuur 6 Routers P2 - Longlist 10
Figuur 7 Routers P3 - Longlist 11
Figuur 8 Cisco SG100 12
Figuur 9 Linksys LGS124 12
Figuur 10 Netgear ProSafe JGS524 12
Figuur 11 Switches P1 - Shortlist 13
Figuur 12 Cisco SG200-50 14
Figuur 13 Cisco SG300-28 14
Figuur 14 Cisco SG500-28 15
Figuur 15 Netgear Prosafe GSM7224 15
Figuur 16 Switches P2 - Shortlist 16
Figuur 17 SG500 /SG500X 17
Figuur 18 Cisco Catalyst 2960S-48TS-L 17
Figuur 19 HP 2910al-48 voor- en achterzijde 18
Figuur 20 HP2920-48g 18
Figuur 21 Switches P3 - Shortlist 19
Figuur 22 Cisco RV110w 20
Figuur 23 Cisco RV320 21
Figuur 24 Draytek Vigor 2130 21
Figuur 25 Draytek 2925Vn+ 21
Figuur 26 Linksys EA6900 22
Figuur 27 Routers P1 - Shortlist 23
Figuur 28 Cisco ASA5505 24
Figuur 29 Fortigate 40C 24
Figuur 30 Watchguard XTM26 24
Figuur 31 Zyxel USG110 25
Figuur 32 Routers P2 - Shortlist 26
Figuur 33 Sonicwall NSA 2600 27
Figuur 34 Fortigate 80CM voor- en achter 27
Figuur 35 Watchguard XTM330 28
Figuur 36 Watchguard XTM 33 28
Figuur 37 Watchguard XTM 525 28
Figuur 38 Routers P3 - Shortlist 29
Figuur 39 Resultaten onderzoek in cocnept building block vorm 30

BRONNEN

Alani, M. M. (2014). *Guide to OSI & TCP/IP Models.*

Cisco. (2008). *Cisco Netflow productinfo*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/flexible-netflow/product_data_sheet0900aecd804b590b.pdf

Cisco. (2012). *Cisco Rv110W productinfo*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/routers/rv110w-wireless-n-vpn-firewall/data_sheet_c78-660141.pdf

Cisco. (2012). *Cisco SG100 productinfo*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/switches/small-business-smart-switches/datasheet_C78-582017.pdf

Cisco. (2013). *Cisco Catalyst 2960s productinfo*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.pdf

Cisco. (2013). *Cisco Catalyst 2960X productinfo*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.pdf

Cisco. (2013). *Cisco RV320 productinfo*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/routers/rv320-dual-gigabit-wan-vpn-router/data_sheet_c78-726132.pdf

Cisco. (2013). *Cisco SG200 productinfo*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/switches/small-business-100-series-unmanaged-switches/data_sheet_c78-634369.pdf

Cisco. (2013). *Cisco SG300 productinfo*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/switches/small-business-smart-switches/data_sheet_c78-610061.pdf

Cisco. (2013). *Cisco SG500 product info*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/switches/small-business-500-series-stackable-managed-switches/c78-695646_data_sheet.html

Cisco. (2013). *Cisco SG500(X) productinfo*. Retrieved from http://www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-500-series-stackable-managed-switches/c22-695647_prod_ov.pdf

Cisco. (2014). *Cisco ASA 5505 productinfo*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-701253.pdf

Dell. (2013). *SonicWall 2600 productinfo*. Retrieved from http://marketing.sonicwall.com/documents/sonicwall-network-security-appliance-series-datasheet-24541.pdf

Draytek. (n.d.). *Draytek 2130 productinfo*. Retrieved from http://www.draytek.nl/files/1-Vigor%202130.pdf

Draytek. (n.d.). *Draytek 2925vn+ productinfo*. Retrieved from http://www.draytek.nl/files/Vigor%202925%20serie.pdf

Fortinet. (2013). *Fortigate 40C productinfo*. Retrieved from http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-40C.pdf

Fortinet. (2013). *Fortigate 80CM productinfo*. Retrieved from http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-80CM.pdf

HP. (2013, 12 12). *HP 2910AL productinfo*. Retrieved from http://h17007.www1.hp.com/us/en/networking/products/switches/HP_2910_al_Switch_Series/index.aspx#.VFn0LfnF-z4

HP. (2013). *HP 2920 Productinfo*. Retrieved from http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA4-5213ENW&doctype=data%20sheet&doclang=EN_US&searchquery=&cc=nl&lc=nl

Linksys / Belkin international. (2013). *LGS124 productinfo*. Retrieved from http://downloads.linksys.com/downloads/datasheet/25820_Belkin_Linksys_Unmanaged_Switches_16_24_Port_PROD.pdf

Linksys. (n.d.). *Linksys EA6900 productinfo*. Retrieved from http://www.linksys.com/nl-eu/products/routers/EA6900

Netgear. (2009). *Netgear GSM724 productinfo*. Retrieved from http://www.downloads.netgear.com/files/gsm7224-gsm7248v2_ds_18feb10.pdf

Netgear. (n.d.). *Netgear JGS524 productinfo*. Retrieved from http://www.downloads.netgear.com/files/GDC/datasheet/en/JGS516v2-JGS524v2.pdf

Watchguard. (2014). *Watchguard APT-blocker module*. Retrieved from Watchguard.com: http://Watchguard.com/wgrd-products/security-modules/apt-blocker

Watchguard. (2014). *Watchguard XTM26 productinfo*. Retrieved from http://Watchguard.com/docs/datasheet/wg_xtm2_ds.pdf

Watchguard. (2014). *Watchguard XTM3 series productinfo*. Retrieved from http://www.Watchguard.com/docs/datasheet/wg_xtm3_ds.pdf

Watchguard. (2014). *Watchguard XTM5 series productinfo*. Retrieved from http://www.Watchguard.com/docs/datasheet/wg_xtm5_ds.pdf

Zyxel. (2014). *Zyxel USG110 productinfo*. Retrieved from ttp://www.zyxel.com/nl/nl/products_services/zywall_1100_310_110.shtml?t=p

Testplan

Constant IT

13 november 2014, Chris de Keijzer
Opleiding: System & Network engineering
Studentnummer: 1591134
Telefoonnummer: 06-10181296
Versie: 1.1

DOCUMENTINFORMATIE

Documentbeheer en Goedkeuring

Versie	Auteur	Opmerkingen	Document Eigenaar	Datum
0.1	Chris de Keijzer	Inhoud	Chris de Keijzer	14-11-2014
0.2	Chris de Keijzer	Inhoud	Chris de Keijzer	18-11-+2014
1.0	Chris de Keijzer	Feedback Chris Leicher verwerkt	Chris de Keijzer	23-11-2014
1.1	Chris de Keijzer	Feedback Chris Leicher verwerkt	Chris de Keijzer	26-11-2014

Dit document is beoordeeld door

Versie	Naam	Functie	Datum beoordeling
0.2	Chris Leicher	Docentbegeleider	21-11-2014
1.0	Chris Leicher	Docentbegeleider	26-11-2014

Dit document is goedgekeurd door

Versie	Naam	Functie	Datum beoordeling

INHOUDSOPGAVE

Inhoudsopgave 3
Verklarende woordenlijst 4
1 Inleiding 6
1.1 Project en projectdoelstelling 6
2 Infrastructuur 7
2.1 Beschikbare apparaten 7
2.2 Beschikbare tools 8
3 Testpunten 9
3.1 Risicoclassificatie 10
4 Hoe wordt er getest 12
5 Testgevallen en testcase 12
5.1 Firewall testgevallen 13
5.2 Switches testgevallen 24
5.3 Testcase: malware blokkeren 33
5.3.1 Uitvoeren testcase 34
6. Conclusie 39
Bronnenlijst 41
Bijlage 43
Bijlage 1 Functioneel ontwerp 43
Bijlage 2 Technisch ontwerp 44

VERKLARENDE WOORDENLIJST

ACL	Access Control Lists welke via regels toegang geven of ontzeggen tot bepaalde netwerkbronnen.
All-in-one oplossing	Één oplossing die voorziet in alle behoefte, binnen het project wordt hiermee een firewall bedoeld die ook dienst kan doen als router.
Best of breed services	Watchguard gebruikt deze term voor hun optionele services, deze worden geleverd door fabrikanten die naar de maning van Watchguard het beste zijn in wat ze doen.
CLI	Command Line Interface waarmee via tekstinvoer commando's aan apparatuur wordt doorgevoerd.
Dual WAN	Dual WAN apparatuur heft twee ingangen voor WAN verbindingen en kan deze simultaan gebruiken.
Definities (malware)	Virusscanners/ malwarescanners maken gebruik van handtekeningen of definities om bepaalde malware te detecteren. De malware wordt dus geïdentificeerd aan de hand van een definitie.
High availability	Een oplossing die altijd beschikbaar is doordat er failover en clustering gebruikt wordt.
Java	Software van een derde partij die in sommige gevallen noodzakelijk is om bepaalde scripts op webpagina's te draaien.
LAN	Local Area Network, dit is het eigen interne netwerk
Layer2	Hiermee wordt layer 2 van het OSI model bedoeld. Veel switches werken op deze laag en kennen dus geen IP adressen maar alleen "frames" en switching gebeurd op basis van MAC adres. (Alani, 2014)
Layer3	Layer 3 is de laag waarop routers en logische paden ofwel routing tables hun werk doen. Deze voorzien in routes op IP basis naar andere netwerkapparatuur. (Alani, 2014)
Longlist	Een lijst met producten die voldoen aan de globale requirements.
Managed switch	Een switch die zoals de naam zegt tot in detail in te stellen valt.
Out of the box	Iets dat werkt zonder dat daar iets voor gedaan hoeft te worden.
QoS	Quality of Service gaat om het garanderen van bepaalde services op het netwerk door prioriteiten te stellen. Denk bijvoorbeeld aan VoIP verkeer dat stabiel moet blijven.
Requirements	De eisen, voor di project zijn deze eerder gedefinieerd in het requirements document.
Shortlist	Een lijst met apparaten die aan eisen en wensen voldoen en waar eventueel goede ervaringen mee zijn. Deze voorkeurslijst is gebaseerd op de longlist
Sizing	Deze term houdt in dat apparatuur passend moet zijn bij een klantcategorie. Denk aan voldoende poorten/doorvoersnelheid.

Smart switch	Een smart switch vult het gat tussen unmanaged en managed switches. Het is een semi-managed switch welke eigenschappen heeft van allebei.
Stacking	Het stapelen van apparatuur, door stacking kunnen twee apparaten (of meer) samenwerken als één.
Subscription based licensing	Dit is het verkrijgen van licenties waarvoor jaarlijks of maandelijks betaald dient te worden. Dit komt vaak voor bij apparatuur die vaak geupdate dient te worden.
Unmanaged switch	Een switch die uit de box werkt, er valt niets in te stellen en functioneert nadat de stekker is ingeplugd.
VoIP	Het Voice over Internet Protocol is bellen via het netwerk.
VPN	Een Virtual Private Network is een verbinding die via het internet (WAN) naar een andere locatie loopt waarmee het lijkt alsof er in het LAN gewerkt wordt. Deze verbindingen zijn veelal versleuteld.
VRRP + bron	
WAN	Met een Wide Area Network wordt het internet bedoeld.
Zero day malware	Malware die net op het publieke web verschenen is, hier zijn geen definities voor en komen dus ongezien voorbij viruscanners.

1 INLEIDING

Dit document heeft als doel de proof of concept (PoC) tests te beschrijven.
Allereerst zal er in de rest van dit hoofdstuk teruggekeken worden op de opdracht en waarom hier een PoC gedaan moet worden. In hoofdstuk twee wordt de apparatuur en tools besproken waarmee getest wordt en in hoofdstuk drie worden de testpunten beschreven. Vervolgens wordt in hoofdstuk vier uitgelegd hoe de verschillende punten getest worden gevolgd door een beschrijving van de testgevallen in hoofdstuk vijf. De figuren in hoofdstuk 5 dienen ingevuld te worden door de tester welke leiden tot de conclusie in hoofdstuk 6.

1.1 PROJECT EN PROJECTDOELSTELLING

Dit project heeft als doelstelling om een productvergelijking te maken van switches, routers en firewalls. Deze apparaten zijn eerst aan een theoretische test onderworpen in de vorm van een longlist en shortlist. Van de apparaten die het best uit de theoretische test komen wordt er een proof of concept opgezet waarmee getest wordt
Dit testplan sluit aan bij het plan van aanpak genaamd: Plan van aanpak standaardisatie Constant IT

2 INFRASTRUCTUUR

Dit hoofdstuk beschrijft de gebruikte apparatuur en infrastructuur binnen het PoC.

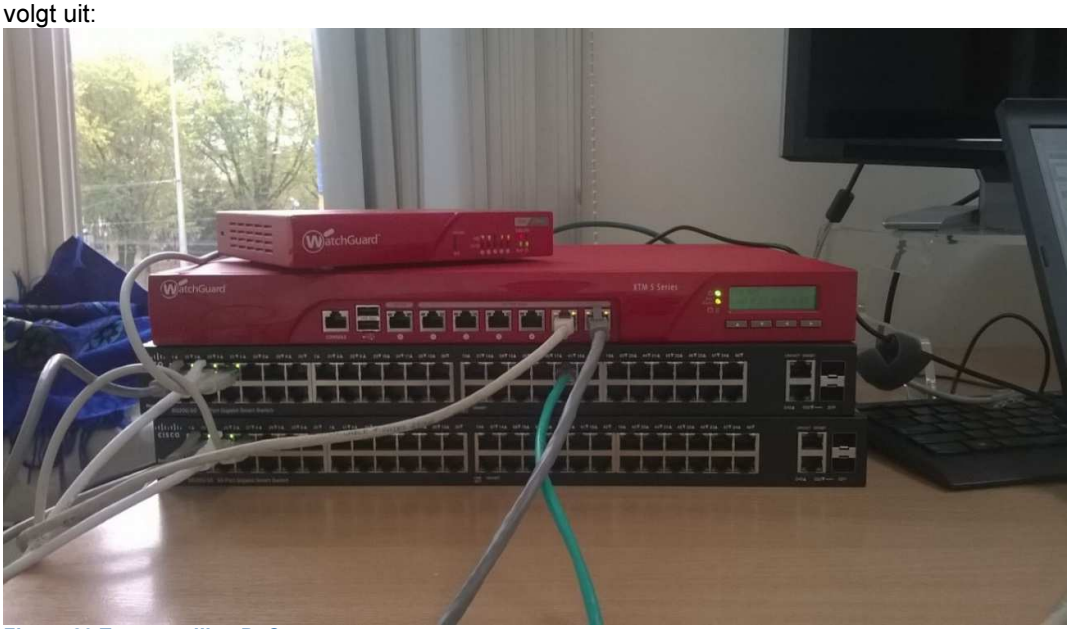
2.1 BESCHIKBARE APPARATEN

Er zijn met behulp van Constant IT een aantal apparaten geregeld waarmee getest kan worden in dit PoC, dit zijn:

- Watchguard XTM 26 welke als beste uit de test kwam voor firewalls in de P2 categorie.
- Twee Cisco SG200 switches welke helaas niet als beste uit de test kwamen in de P2 categorie maar qua layer 2 functionaliteiten en hardware compleet gelijk is aan de SG300.
- Watchguard XTM 505 welke niet aan tests zal worden onderworpen en alleen gebruikt wordt voor connectiviteit.

De complete omgeving wordt volgens “best practices” opgebouwd die door de fabrikant gesteld zijn. Voor Watchguard firewalls is hiervoor een driedaagse basistraining gedaan welke voldoende is om alle testgevallen te kunnen uitvoeren, hiervoor is ook een PDF bestand beschikbaar gesteld door Watchguard[15]. Cisco switches worden opgebouwd op de wijze die beschreven staat in de documentatie op de Cisco website[16]. Daarnaast zal de bedrijfslaptop dienst doen als zowel client voor het verzenden van data over de infrastructuur als logserver voor het ontvangen van berichten van de Watchguard firewall(s).

Het PoC dat opgebouwd is volgens het technisch ontwerp dat te vinden is in de bijlage ziet er als volgt uit:



Figuur 83 Testopstelling PoC

[15] https://www.dropbox.com/s/wu7rlfdtmn5t19i/Fireware-Essentials_v11-9-3.pdf?dl=0
[16] https://www.dropbox.com/s/2yz9nku2oqp1a5j/Sg300%20technical%20documentation.pdf?dl=0

2.2 BESCHIKBARE TOOLS

Voor het testen is vastgesteld dat minimaal de volgende tools nodig zijn:

- Watchguard system manager waarmee één of meerdere Watchguards beheerd kunnen worden vanaf de lokale computer;
- Watchguard Logserver welke firewall meldingen zal registreren wat handig is bij het testen en bij het opzetten van de omgeving;
- Een tool om verkeer te generen zoals bijvoorbeeld de UDP flood generator van Startrinity[17], deze is nodig om doorvoersnelheden te testen;
- Een tool om een overduidelijke DOS aanval te genereren zoals LOIC[18], deze is nodig om tests met betrekking tot (D)DDOS aanvallen te doen;
- Een tool om legitiem verkeer mee te creëren om belasting te generen.[19], welke nodig is om een constante maar ook realistische belasting op bepaalde onderdelen creëren;
- Een programma om schermafbeeldingen mee te maken, hiervoor wordt de ingebouwde “snipping tool” van Windows gebruikt.

[17] http://startrinity.com/VoIP/NetworkTester/NetworkTester.aspx
[18] http://sourceforge.net/projects/loic/
[19] https://www.softether.org/4-docs/1-manual/4._SoftEther_VPN_Client_Manual/4.8_Measuring_Effective_Throughput

3 TESTPUNTEN

In dit hoofdstuk worden de punten beschreven die getest worden in het PoC. Deze zijn gebaseerd op de zaken waaraan voldaan werd in het onderzoek. Aan de hand van de TMAP methode worden een aantal kwaliteitsattributen onderkend. De mogelijke attributen zijn: beschikbaar, schaalbaar, veilig, aanpasbaar, beheerbaar en toerekenbaar.
(Horsten, 2012)
De testpunten komen later terug in de testrapportage als testgevallen die in hoofdstuk 5 beschreven worden.

	Niveau eisen	Testpunten firewall (Watchguard XTM26)	Kwaliteitsattribuut TMAP
1	Must	Multi wan (failover of bundelen)	Beschikbaar
2	Must	Gigabit poorten	Schaalbaar
3	Must	IPv6	Aanpasbaar
4	Must	Link aggregation	Schaalbaar
5	Could	Uitbreidbaarheid via licenties	Schaalbaar
6	Must	Loggen via webinterface, syslog of mail.	Beheerbaar
7	Should	Reporting op basis van vooraf ingestelde paramaters	Beheerbaar
8	Must	Site to site VPN	Beschikbaar
9	Must	Voldoende VPN troughput	Beschikbaar
10	Must	VPN failover	Beschikbaar
11	Must	Qos & Traffic management/shaping	Beschikbaar
12	Must	DHCP	Schaalbaar
13	Must	SNMP	Beheerbaar
14	Must	Verschillende NAT types (specifiek NAT loopback)	Aanpasbaar
15	Should	LDAP/AD integratie	Veilig
16	Must	IPsec	Veilig
17	Must	VLAN support	Veilig
18	Must	ACL's	Veilig
19	Should	DDOS herkenning.	Veilig
20	Could	IDS/IPS	Veilig
21	Could	Security levels instellen	Toerekenbaar
22	Could	Audit logs	Toerekenbaar

Figuur 84 Testpunten firewall

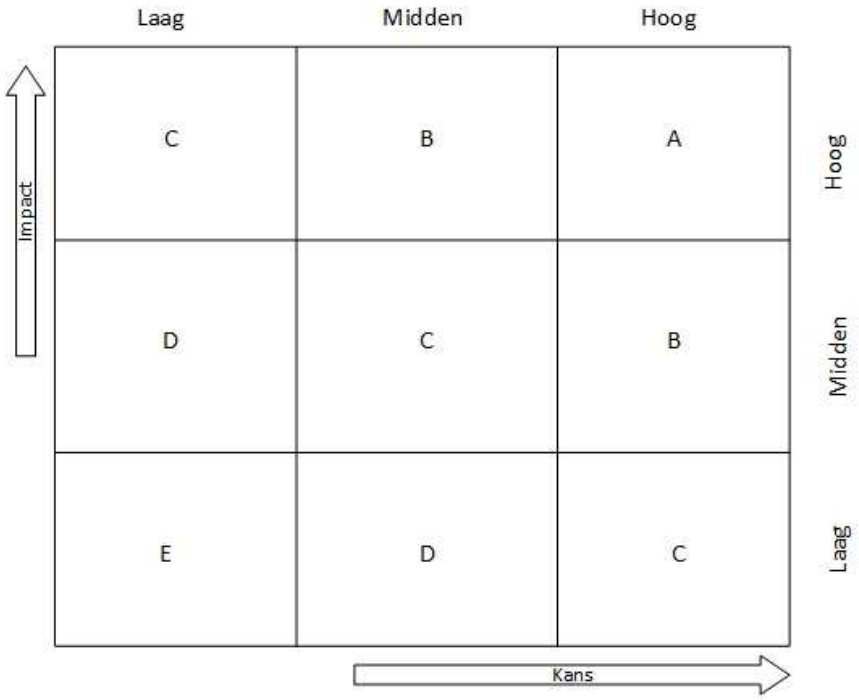
	Niveau eisen	Testpunten SG200	Kwaliteitsattribuut TMAP
1	Must	Ipv6	Aanpasbaar
2	Must	1 Gbit interfaces	Schaalbaar
3	Should	Mogelijkheden tot failover	Beschikbaar
4	Must	Loggen via webinterface, syslog of mail.	Beheerbaar
5	Must	Backup en export van configs	Beheerbaar
6	Must	Remote access via telnet, ssh, web, tool.	Beheerbaar
7	Should	Diagnostische tools	Beheerbaar
8	Must	Etherchannel(LACP)	Schaalbaar
9	Must	QoS	Beschikbaar
10	Must	LLDP	Schaalbaar
11	Must	SNMP	Beheerbaar
12	Must	VLAN (en VTP)	Veilig

Figuur 85 Testpunten switches

Naast de testpunten is er ook een voor Constant IT relevante testcasus ontworpen, hierover valt alles te lezen in hoofdstuk 5.1

3.1 RISICOCLASSIFICATIE

Om de tests voorspoedig te laten verlopen, moeten de risico's bij het testen in kaart gebracht worden. Deze zogenoemde risicoclassificatie vormt de basis voor de teststrategie en moet gedaan worden voor ieder testpunt. Om de risicoclassificatie te verkrijgen wordt de volgende formule gebruikt: Risico = faalkans x impact. (Horsten, 2012) De faalkans is de kans dat er een fout of probleem optreedt en de impact zegt iets over de schade die een fout of probleem kan veroorzaken. De tests die een classificatie hebben van A t/m D worden uitgevoerd. Tests met de classificatie E blijven achterwege



Figuur 86 Risicoclassificatie tabel

In de tabellen hieronder worden de risico's geclassificeerd, de eerste tabel bevat de risico's van de firewall (Watchguard XTM26) en de tweede tabel bevat die van de switches (SG200)

	Productrisico	Kans	Impact	Classificatie
1	Multi wan (failover of bundelen)	Middel	Hoog	B
2	Gigabit poorten	Laag	Hoog	C
3	IPv6	Laag	Hoog	C
4	Link aggregation	Middel	Middel	C
5	Uitbreidbaarheid via licenties	Laag	middel	D
6	Loggen via webinterface, syslog of mail.	Laag	Hoog	C
7	Reporting op basis van vooraf ingestelde paramaters	Middel	Middel	C
8	Site to site VPN	Laag	Hoog	C
9	Voldoende VPN troughput	Laag	Hoog	C
10	VPN failover	Hoog	Hoog	A
11	Qos & Traffic management/shaping	Laag	Middel	D
12	DHCP	Laag	Hoog	C
13	SNMP	Laag	Laag	E
14	Verschillende NAT types (specifiek NAT loopback)	Laag	Middel	D
15	LDAP/AD integratie	Laag	Laag	E
16	IPsec	Middel	Hoog	B
17	VLAN support	Laag	Hoog	C
18	ACL's	Laag	Hoog	C
19	DDOS herkenning.	Middel	Hoog	B
20	IDS/IPS	Laag	Hoog	C
21	Security levels instellen	Laag	Middel	D
22	Audit logs	Hoog	Laag	C

Figuur 87 Risicoclassficatie firewall

	Productrisico	Kans	Impact	Classificatie
1	Ipv6	Laag	Hoog	C
2	Gbit interfaces	Laag	Hoog	C
3	Mogelijkheden tot failover	Middel	Hoog	B
4	Stacking	Laag	Middel	D
6	Loggen via webinterface, syslog of mail.	Middel	Middel	C
7	Backup en export van configs	Laag	Hoog	C
8	Remote access via telnet, ssh, web, tool.	Laag	Hoog	C
9	Notificaties (send mail when down)	Laag	Laag	E
10	Reporting op basis van vooraf ingestelde paramaters	Laag	Laag	E
11	Console Port	Laag	Midden	D
12	Diagnostische tools	Middel	Middel	C
13	Opties voor centraal beheer	Laag	Laag	E
14	Etherchannel(LACP)	Laag	Hoog	C
15	QoS	Middel	Middel	C
16	LLDP	Laag	Laag	E
17	SNMP	Laag	Laag	E
18	Layer 3 functionaliteit	Hoog	Middel	B
19	VLAN	Laag	Hoog	C
20	VLAN verspreiding	Hoog	Middel	B
21	Security levels instellen	Middel	Middel	C
22	ACL	Hoog	Laag	C

Figuur 88 Risicoclassficatie switches

4 HOE WORDT ER GETEST

Dit hoofdstuk beschrijft welke testontwerptechnieken worden gebruikt bij het testen van de verschillende testpunten.

• Controlelijsten welke gebruikt warden om aanwezigheid van bepaalde mogelijkheden te verifiëren
• Logging of rapportage controleren wordt voornamelijk gebruikt bij duurtesten of testen die een mogelijk fout opleveren
• Real-life test waarmee geprobeerd word een real life scenario te schetsen, deze is veelal gecombineerd met de vrije vorm tests.
• Vrije vorm voor het testen van real life scenario's, deze is gebaseerd op het technisch ontwerp. Het doel van deze test is het controleren of de interactie tussen de verschillende onderdelen naar behoren werkt
• Exploratory testen waarmee zowel geleerd als getest wordt, dit kan lijden tot nieuwe testgevallen.

5 TESTGEVALLEN EN TESTCASE

De testgevallen worden in dit hoofdstuk beschreven. Testgevallen worden opgeleverd aan de technisch expert die de testen gaat uitvoeren met een korte omschrijving. Elk testgeval wordt afgerond met een "OK" of "NOK" met eventuele toelichting of screenshots van een meetbare waarde..

Hoofdstuk 5.1 bevat een scenario dat op dit moment speelt binnen Constant IT. Het doel van dit scenario is om aan te tonen dat de Watchguard firewall malware infecties kan tegen houden.

5.1 FIREWALL TESTGEVALLEN

Nummer	F1 - Multi WAN (failover of bundelen)
Omschrijving test	Check werking multi-wan, wat zijn de tijden totdat de failover inschakelt. Is er ook een mogelijkheid tot fallback?
Tester	Chris
Fase	PoC
Precondities	Operationele PoC omgeving met (gesimuleerde) WAN verbinding.
Handelingen	Opzetten multi WAN, testen wat er gebeurd wanneer de verbinding verloren gaat
Toelichting	
Verwachte uitkomst	OK. Failover werkt, fallback mogelijk niet.
Resultaat	OK, failover en fallback werken beiden. Er valt zelfs in te stellen dat verkeer meteen weer de primaire verbinding gebruikt of dat er langzaam wordt overgegaan.
Datum test	14-11-2014
Maatregel	

Figuur 89 Multi WAN testgeval

Nummer	F2 - Gigabit poorten
Omschrijving test	
Tester	Chris
Fase	PoC
Precondities	Aanwezigheid apparaat
Handelingen	Interfaces controleren
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK
Datum test	14-11-2014
Maatregel N.v.t.	

Figuur 90 Gigabit poorten testgeval

Nummer	F3 - IPv6
Omschrijving test	
Tester	Chris
Fase	PoC
Precondities	Operationeel apparaat
Handelingen	Een stuk netwerk maken met IPv6.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, er kan ook een dual stack gemaakt worden met IPv4 en 6
Datum test	14-11-2014
Maatregel	

Figuur 91 IPv6 testgeval

Nummer	F4 - Link aggregation
Omschrijving test	
Tester	Chris
Fase	PoC
Precondities	Operationeel apparaat
Handelingen	Links bundelen op firewall bundelen naar switch.
Toelichting	
Verwachte uitkomst	OK.
Resultaat	OK, dit werkt op de firewall anders dan verwacht. Er wordt eerst een link aggregation group gemaakt waar vervolgens interfaces aan toegevoegd worden.
Datum test	14-11-2014
Maatregel	

Figuur 92 Link aggregation testgeval

Nummer	F5 - Uitbreidbaarheid via licenties
Omschrijving test	
Tester	Chris
Fase	PoC
Precondities	Aanwezigheid apparaat.
Handelingen	Controleer aan de hand van de feature lijst van het apparaat of daar uitbreiding voor te krijgen zijn.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, aankoop van licenties wordt opgeslagen in de cloud. Apparaten kunnen hun “feature key” synchroniseren met de cloud. Als er geen wens is om cloud functionaliteit te gebruiken kan een “feature key” ook offline geïmporteerd worden
Datum test	14-11-2014
Maatregel	

Figuur 93 Uitbreidbaarheid via licenties testgeval

Nummer	F6 - Loggen via webinterface, syslog of mail.
Omschrijving test	
Tester	Chris
Fase	PoC
Precondities	Werkende PoC omgeving Log Server
Handelingen	Log server en systemen opzetten volgens technisch ontwerp opzetten
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, er is gebruik gemaakt van een lokale installatie van Watchguard system manager welke ook een logging functie heeft.
Datum test	14-11-2014
Maatregel	

Figuur 94 Loggen testgeval

Nummer	F7 - Reporting op basis van vooraf ingestelde paramaters
Omschrijving test	Onderzoek de mogelijkheid tot rapportages. Zijn deze vooraf in te stellen?
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd Log Server (Mogelijk Watchguard Dimension server noodzakelijk)
Handelingen	Logs generen en rapport uit draaien.
Toelichting	
Verwachte uitkomst	NOK, extra kosten verbonden aan plug-in
Resultaat	OK onder voorbehoud, er vallen met Dimension rapportages uit te draaien. Echter valt niet te plannen dat dit een terugkerende actie moet zijn. Elk rapport dient handmatig gemaakt te worden.
Datum test	14-11-2014
Maatregel	

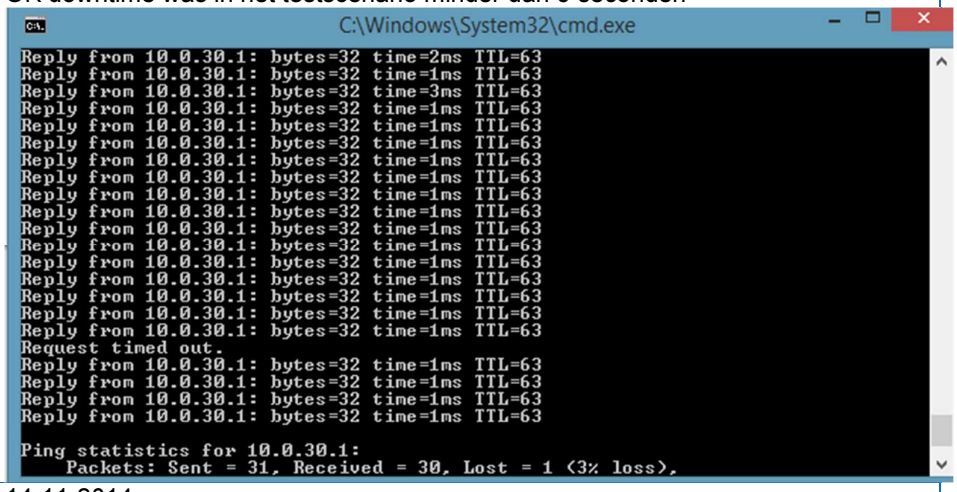
Figuur 95 Reporting testgeval

Nummer	F8 - Site to site VPN
Omschrijving test	
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd met WAN mogelijkheid.
Handelingen	VPN tunnel maken.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK. Om een VPN te maken moet er eerst een gateway gemaakt worden, daarna wordt er een branche office VPN (BOVPN) gemaakt.
Datum test	14-11-2014
Maatregel	

Figuur 96 Site-to-site testgeval

Nummer	F9 - Voldoende VPN troughput
Omschrijving test	
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd Log server
Handelingen	Tunnel opzetten tussen locaties. Routeren internet verkeer via locatie 1
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, er wordt geadverteerd met 40Mbps troughput en er werd 42Mbps gehaald.
Datum test	14-11-2014
Maatregel	

Figuur 97 VPN troughput testcase

Nummer	F10 - VPN failover
Omschrijving test	Het doel van deze test is om VPN failover te testen. De VPN loopt over twee WAN verbindingen, wat betekend dat als de verbinding verloren wordt op één verbinding de andere het zou moeten overnemen. De vraag is of de VPN dit automatisch doet.
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd met WAN mogelijkheid.
Handelingen	VPN tunnel maken via meerdere WAN interfaces.
Toelichting	Bij verlies verbinding van een WAN interface moet de tunnel blijven functioneren. Er moet ook een tijdschatting gemaakt worden van de tijd totdat de tunnel weer werkt.
Verwachte uitkomst	OK
Resultaat	OK downtime was in het testscenario minder dan 5 seconden 
Datum test	14-11-2014
Maatregel N.v.t.	

Figuur 98 VPN failover testgeval

Nummer	F11 - Qos & Traffic management/shaping
Omschrijving test	
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd
Handelingen	QoS instellen op een interface.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK
Datum test	14-11-2014
Maatregel	

Figuur 99 QoS testgeval

Nummer	F12 - DHCP
Omschrijving test	Werkt DHCP ook in combinatie met VLANs?
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd
Handelingen	DHCP aanzetten op een interface.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, er kunnen meerdere interfaces adressen uit één scope halen.
Datum test	14-11-2014
Maatregel	

Figuur 100 DHCP testgeval

Nummer	F13 - Verschillende NAT types (specifiek NAT loopback)
Omschrijving test	
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd
Handelingen	
Toelichting	
Verwachte uitkomst	OK, handleiding raadplegen voor configuratie i.v.m best practice
Resultaat	OK, er kan een extern IP via NAT bereikt worden terwijl er in het LAN gewerkt wordt.
Datum test	14-11-2014
Maatregel	

Figuur 101 NAT testgeval

Nummer	F14 - LDAP/AD integratie
Omschrijving test	Controleer de mogelijk tot integratie, er is geen server beschikbaar om mee te testen
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd
Handelingen	
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, users aanmaken op basis van LDAP/AD kan.
Datum test	14-11-2014
Maatregel	

Figuur 102 LDAP/AD testgeval

Nummer	F15 - IPsec
Omschrijving test	Er moet getest worden of IPsec kan en hoe/of het voldoende werkt.
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd
Handelingen	VPN opzetten waarbij deze optie geselecteerd wordt.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK
Datum test	14-11-2014
Maatregel N.v.t.	

Figuur 103 IPsec testgeval

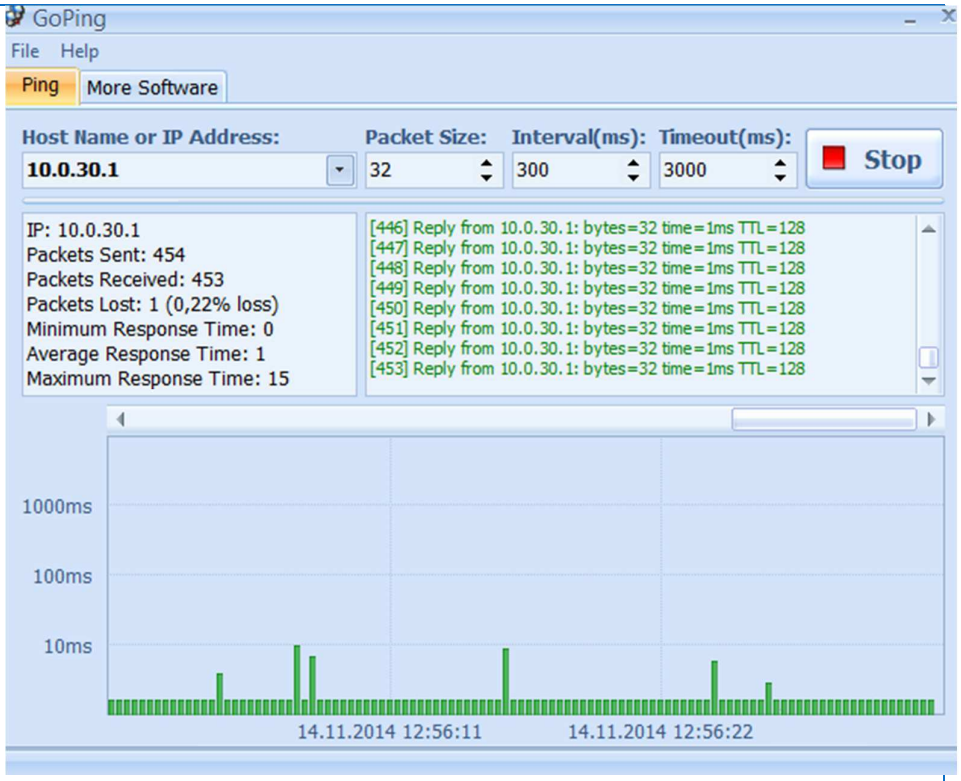
Nummer	F16 - VLAN support
Omschrijving test	VLANs moeten gerouteerd kunnen worden
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd
Handelingen	Volgens het technisch ontwerp doet de firewall intervlan routing, dit moet dus ingesteld worden
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK
Datum test	14-11-2014
Maatregel	

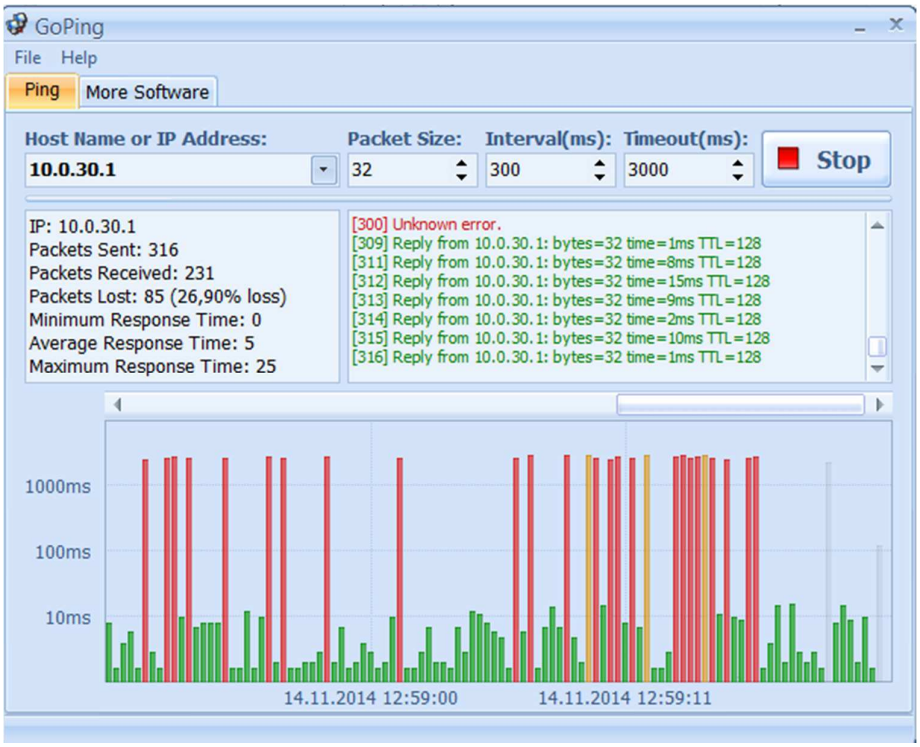
Figuur 104 VLAN testgeval

Nummer	F17 - ACL's
Omschrijving test	Test de mogelijke ACL's, is het mogelijk om specifieke (interne) range te blokkeren?
Tester	Chris
Fase	PoC
Precondities	
Handelingen	Firewall policy maken die een specifieke computer toegang ontzegt
Toelichting	14-11-2014
Verwachte uitkomst	OK
Resultaat	OK, er kan geblokt worden op range, protocol of een enkel IP blacklisten
Datum test	14-11-2014
Maatregel	

Figuur 105 ACL testgeval

Nummer	F18 - DDOS herkenning
Omschrijving test	Test of de firewall automatisch actie onderneemt bij een DDOS aanval.
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd
Handelingen	Gebruik maken van eenvoudige flooding tool om netwerk te testen.
Toelichting	Er wordt een ping over de tunnel gestuurd, met behulp van de tool GoPing kan zeer eenvoudig gezien worden wat voor een impact de flooding heeft.
Verwachte uitkomst	OK
Resultaat	OK, echter kost al het blokkeren van pakketten wel performance. Er is getest met een UDPflood die ongeveer 100Mbit genereerde. Onderstaande figuren geven een inzicht van de impact.


GoPing
File Help
Ping More Software
Host Name or IP Address:
10.0.30.1
Packet Size:
32
Interval(ms):
300
Timeout(ms):
3000
Stop
IP: 10.0.30.1
Packets Sent: 454
Packets Received: 453
Packets Lost: 1 (0,22% loss)
Minimum Response Time: 0
Average Response Time: 1
Maximum Response Time: 15
[446] Reply from 10.0.30.1: bytes=32 time=1ms TTL=128
[447] Reply from 10.0.30.1: bytes=32 time=1ms TTL=128
[448] Reply from 10.0.30.1: bytes=32 time=1ms TTL=128
[449] Reply from 10.0.30.1: bytes=32 time=1ms TTL=128
[450] Reply from 10.0.30.1: bytes=32 time=1ms TTL=128
[451] Reply from 10.0.30.1: bytes=32 time=1ms TTL=128
[452] Reply from 10.0.30.1: bytes=32 time=1ms TTL=128
[453] Reply from 10.0.30.1: bytes=32 time=1ms TTL=128
1000ms
100ms
10ms
14.11.2014 12:56:11
14.11.2014 12:56:22


GoPing
File Help
Ping More Software
Host Name or IP Address:
10.0.30.1
Packet Size:
32
Interval(ms):
300
Timeout(ms):
3000
Stop
IP: 10.0.30.1
Packets Sent: 316
Packets Received: 231
Packets Lost: 85 (26,90% loss)
Minimum Response Time: 0
Average Response Time: 5
Maximum Response Time: 25
[300] Unknown error.
[309] Reply from 10.0.30.1: bytes=32 time=1ms TTL=128
[311] Reply from 10.0.30.1: bytes=32 time=8ms TTL=128
[312] Reply from 10.0.30.1: bytes=32 time=15ms TTL=128
[313] Reply from 10.0.30.1: bytes=32 time=9ms TTL=128
[314] Reply from 10.0.30.1: bytes=32 time=2ms TTL=128
[315] Reply from 10.0.30.1: bytes=32 time=10ms TTL=128
[316] Reply from 10.0.30.1: bytes=32 time=1ms TTL=128
1000ms
100ms
10ms
14.11.2014 12:59:00
14.11.2014 12:59:11


2014-11-14 10:37:39 Deny 10.10.10.110 10.0.30.1 13014/udp 65318 13014 0-Chris BCK interface 3-WAN_POC_1 udp flooding 540 128 (Internal Polic
2014-11-14 10:37:54 sessiond Management user status@Firebox-DB from 10.10.10.110 logged in id="3E00-0002"
2014-11-14 10:37:55 sessiond Management user status@Firebox-DB from 10.10.10.110 logged out id="3E00-0004"
2014-11-14 10:37:59 Deny 10.10.10.110 10.0.30.1 13014/udp 65318 13014 0-Chris BCK interface 3-WAN_POC_1 udp flooding 540 128 (Internal Polic
2014-11-14 10:38:19 Deny 10.10.10.110 10.0.30.1 13014/udp 65318 13014 0-Chris BCK interface 3-WAN_POC_1 udp flooding 540 128 (Internal Polic

Datum test	14-11-2014
Maatregel	Stel firewall policies in op “drop” in plaats van “deny” om snelheid te behouden. Omdat het apparaat geen feedback geeft wanneer er een “drop” plaatsvind hoeft er minder processorkracht gebruikt te worden.

Figuur 106 DDOS herkenning testgeval

Nummer	**F19 - IDS/IPS**
Omschrijving test	Mogelijke indringers moeten worden gedetecteerd.
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd Log server
Handelingen	Een indringer proberen te simuleren door een virus te downloaden. Hiervoor moet eerst een (trial) security bundel geactiveerd worden.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, instellen werkt zeer eenvoudig er moet alleen rekening mee gehouden worden dat definities geupdate worden via het internet. Virussen die nog niet zo lang op het internet circuleren komen door de firewall heen (tenzij er een drop of deny wordt gegeven aan onbekend verkeer)
Datum test	14-11-2014
Maatregel	

Figuur 107 IDS/IPS testgeval

Nummer	**F20 - Security levels instellen**
Omschrijving test	Valt sterk samen met F22, er moeten verschillende gebruikers met verschillende rechten aangemaakt kunnen worden
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd
Handelingen	Test admin gebruiker aanmaken welke een foute configuratie moet uitvoeren.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, echter zijn er maar 2 niveaus beschikbaar namelijk: readonly acces of full access.
Datum test	14-11-2014
Maatregel	

Figuur 108 Security levels testgeval

Nummer	F21 - Audit logs
Omschrijving test	Verschillende gebruikers moeten het systeem kunnen aanpassen, echter zal er wanneer het misgaat ook iemand aan te spreken zijn. De logs moeten kunnen controleren wie een fout gemaakt heeft.
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd Log server
Handelingen	Loggen naar de server en vervolgens onderscheid proberen te maken tussen gebruikers
Toelichting	
Verwachte uitkomst	NOK
Resultaat	OK, er kan inzichtelijk gemaakt worden wat welke gebruiker doet. In de figuur hieronder kan er gezien worden wat administrator Chris doet op de Watchguard. In het geval dat de WAN_POC_1 interface uit zou vallen kan er direct naar Chris gegaan worden om te vragen wat hij gedaan heeft waardoor het probleem sneller wordt opgelost. 
Datum test	14-11-2014
Maatregel N.v.t.	

Figuur 109 Audit logs testgeval

5.2 SWITCHES TESTGEVALLEN

Nummer	S1 - Ipv6
Omschrijving test	Valt het apparaat ook te bereiken via IPv6?
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd.
Handelingen	IPv6 op management interface instellen
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, kan ook via dual stack.
Datum test	14-11-2014
Maatregel N.v.t.	

Figuur 110 Ipv6 testgeval

Nummer	S2 - 1 Gbit interfaces
Omschrijving test	Zijn alle interfaces 1Gbit?
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	Interfaces controleren.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK
Datum test	14-11-2014
Maatregel N.v.t.	

Figuur 111 1Gbt testgeval

Nummer	S3 - Mogelijkheden tot failover
Omschrijving test	Test of interfaces in een failover systeem gezet kunnen worden
Tester	Chris
Fase	PoC
Precondities	Systemen volgens technisch ontwerp opgebouwd
Handelingen	Failover “team” aanmaken.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, het is niet mogelijk om bepaalde links in standby te zetten totdat een andere link uitvalt. Echter wordt er met behulp van het later beschreven LACP wel een vorm van redundantie behaald,
Datum test	
Maatregel	

Figuur 112 Failover testgeval

Nummer	S4 - Stacking.
Omschrijving test	Kan het apparaat een stack opbouwen met een ander?
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	
Toelichting	
Verwachte uitkomst	OK
Resultaat	NOK
Datum test	14-11-2014
Maatregel	

Figuur 113 Stacking - testgeval

Nummer	S5 - Loggen via webinterface, syslog of mail.
Omschrijving test	Controleer of de opties aanwezig zijn. Houdt het apparaat ook lokaal logs bij?
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, er kan naar syslog geschreven worden en de webinterface houdt ook logs bij.
Datum test	14-11-2014
Maatregel	

Figuur 114 Loggen testgeval

Nummer	S6 - Backup en export van configs
Omschrijving test	Kan het systeem configuraties exporten en importen? Is het mogelijk om configuraties te wisselen tussen apparaten van hetzelfde type?
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	Configureer een switch en probeer deze configuratie te laden op een andere switch.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, configuraties kunnen worden geëxploreerd en geïmporteerd via http. Dit werkt eerst wat omslachtig en er moet goed gelezen worden, ook duidelijke instructies ontbreken. Echter functioneert het wel en kunnen configuraties ook van encryptie worden voorzien. Plain tekst configuraties zijn ook te importeren door switches van exact hetzelfde type
Datum test	14-11-2014
Maatregel	

Figuur 115 Backup en export testgeval

Nummer	S7 - Remote access via telnet, ssh, web, tool.
Omschrijving test	Is er een mogelijkheid om het apparaat remote te benaderen.
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	Telnet of SSH aanzetten en verbinden hiermee.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, Na een update van de firmware (1.3.0.62 of hoger) valt dit onder de mogelijkheden
Datum test	14-11-2014
Maatregel	

Figuur 116 Remote access testgeval

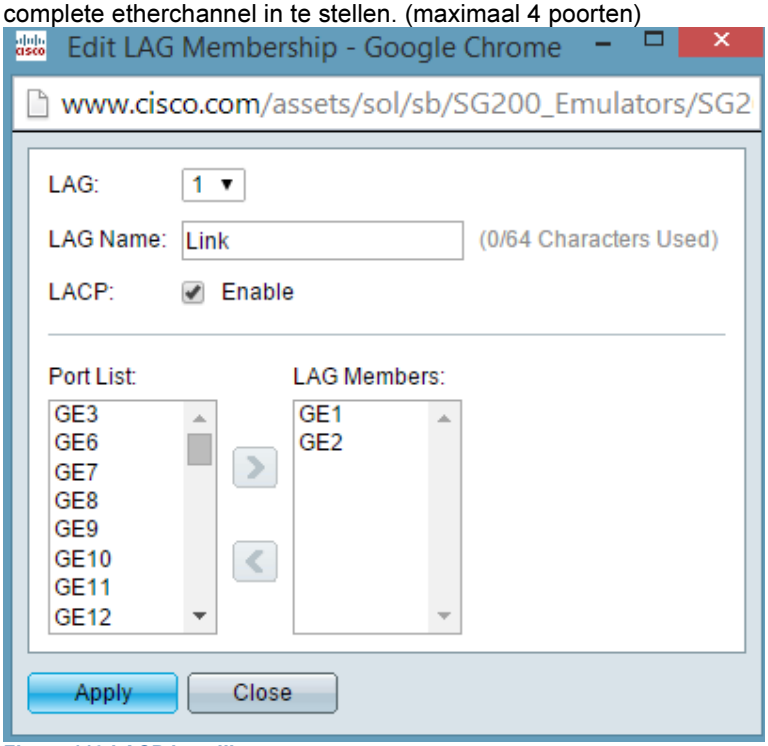
Nummer	S8 - Console port
Omschrijving test	Beschikt het apparaat over een console port?
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, Aanwezig op Cisco SG300 bij klant.
Datum test	14-11-2014
Maatregel	

Figuur 117 Console port - testgeval

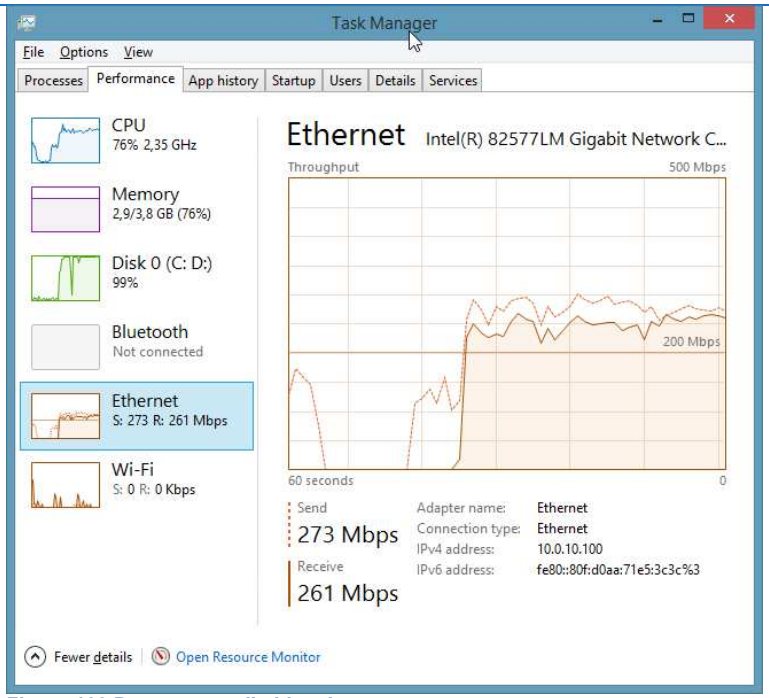
Nummer	S9 - Diagnostische tools
Omschrijving test	Zijn er diagnostische tools op het apparaat aanwezig of via een applicatie die bij het apparaat wordt geleverd.
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	Test de ingebouwde tools, wat is er mogelijk?
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, eenvoudige zaken als zien of er stroom op de lijn staat en ping.
Datum test	
Maatregel	

Figuur 118 Diagnostische tools testgeval

Nummer	S10 - Etherchannel(LACP)
Omschrijving test	Hoe werkt het creëren van een etherchannel, en wat is de snelheid hiervan?
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	Etherchannel maken. Met UDPflood applicatie zoals Starttrinity UDP flooder de doorvoer meten. (StarTrinity, 2014)
Toelichting	Er kan getest worden met behulp van twee laptops en een network flooder. Echter hebben deze maar 1Gbit netwerkaarten waardoor de resultaten tegen kunnen vallen.
Verwachte uitkomst	OK
Resultaat	Het is op Cisco switches met een webinterface zeer eenvoudig om een etherchannel te maken, er valt binnen 5 maal klikken een complete etherchannel in te stellen. (maximaal 4 poorten)



Figuur 119 LACP instellingen



Figuur 120 Doorvoersnerlheid op laptop

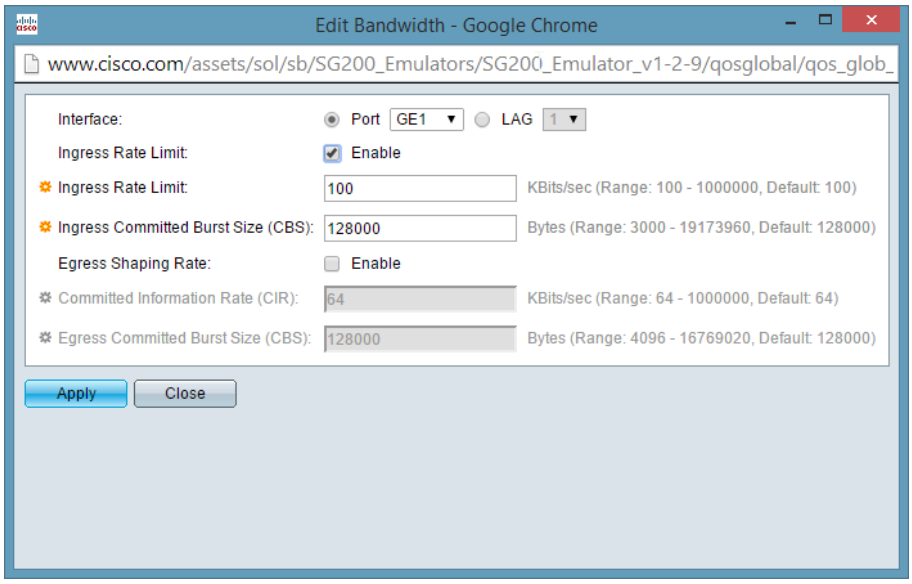
Gedurende 30 seconden is er tussen 2 laptops verkeer geweest zoals in de figuur hierboven. De totale doorvoer was ongeveer 1.1Gbps voordat er tegen de grenzen van de laptops werd aangelopen.

Datum test	14-11-2014
Maatregel	

Figuur 121 Etherchannel testgeval

Nummer	**S11 - QoS**
Omschrijving test	Stel op een aantal interfaces QOS in, is het mogelijk bepaalde zaken te limiteren tot een specifiek aantal KBps of procent.
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	QoS instellen
Toelichting	

Verwachte uitkomst	OK

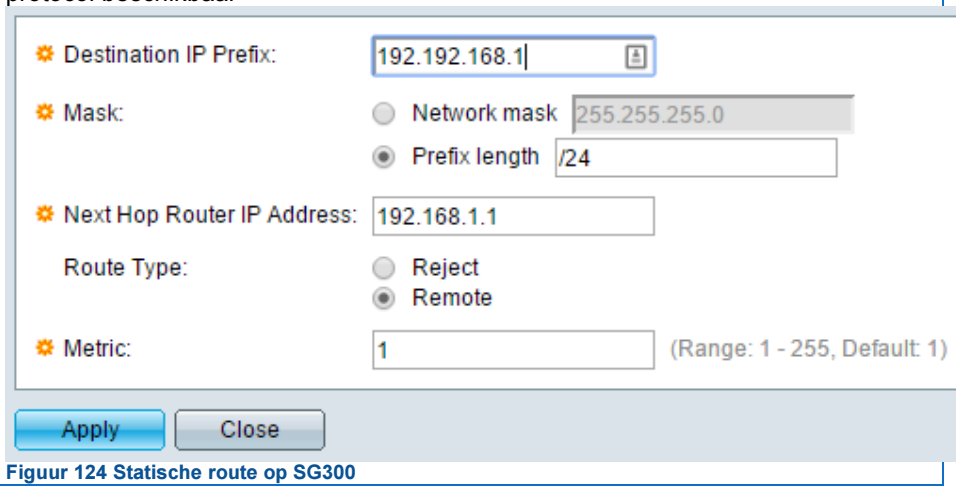


Figuur 122 QoS opties

Resultaat	OK. Er zijn gedetailleerde opties beschikbaar tot het limiteren van bandbreedte echter is dit niet alles want er zijn ook wachtrijen beschikbaar welke meer of minder prioriteit kunnen hebben.
Datum test	
Maatregel N.v.t.	

Figuur 123 QoS testgeval

Nummer	**S12 - Layer 3 functionaliteit**
Omschrijving test	Kan het apparaat op layer 3 werken?
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	Aanzetten layer 3 modus.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, SG300 heeft de mogelijkheid statische routes aan te maken. Er is geen routing protocol beschikbaar



Figuur 124 Statische route op SG300

Datum test	14-11-2014
Maatregel	

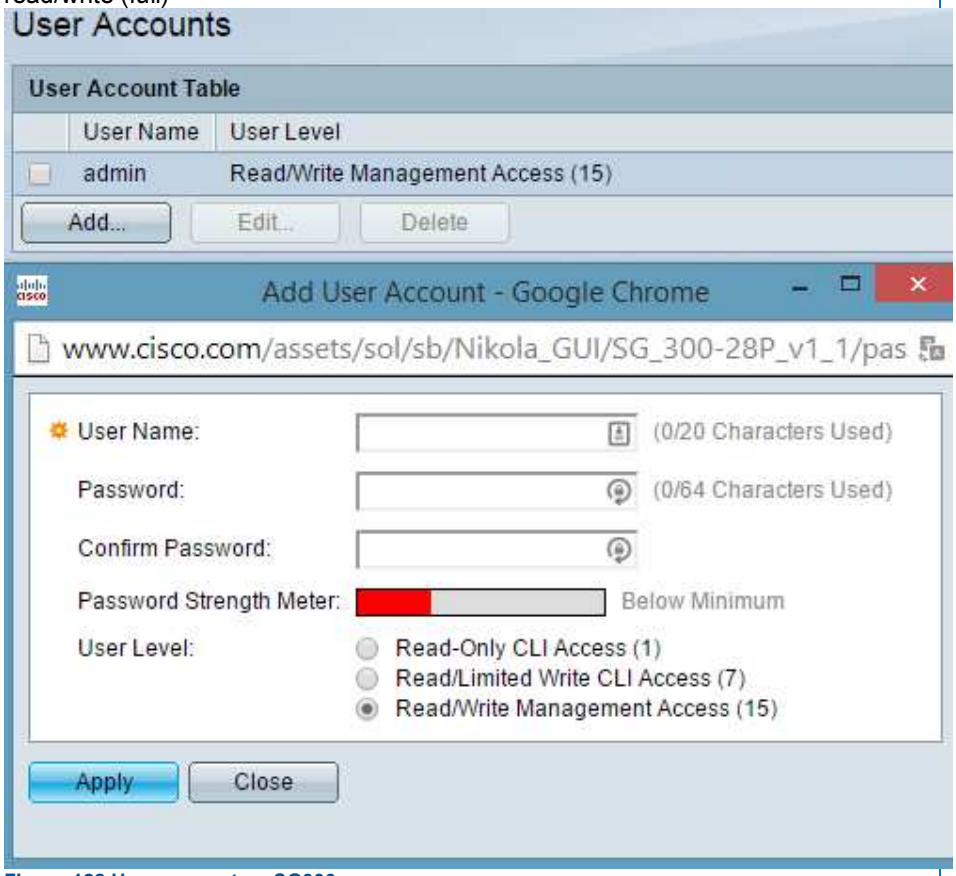
Figuur 125 Layer 3 functionaliteit – testgeval

Nummer	**S13 - VLAN**
Omschrijving test	Kan het apparaat VLANs maken?
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	VLANs aanmaken.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, er kunnen tot 2048 verschillende VLANs gemaakt worden
Datum test	14-11-2014
Maatregel	

Figuur 126 Vlan testgeval

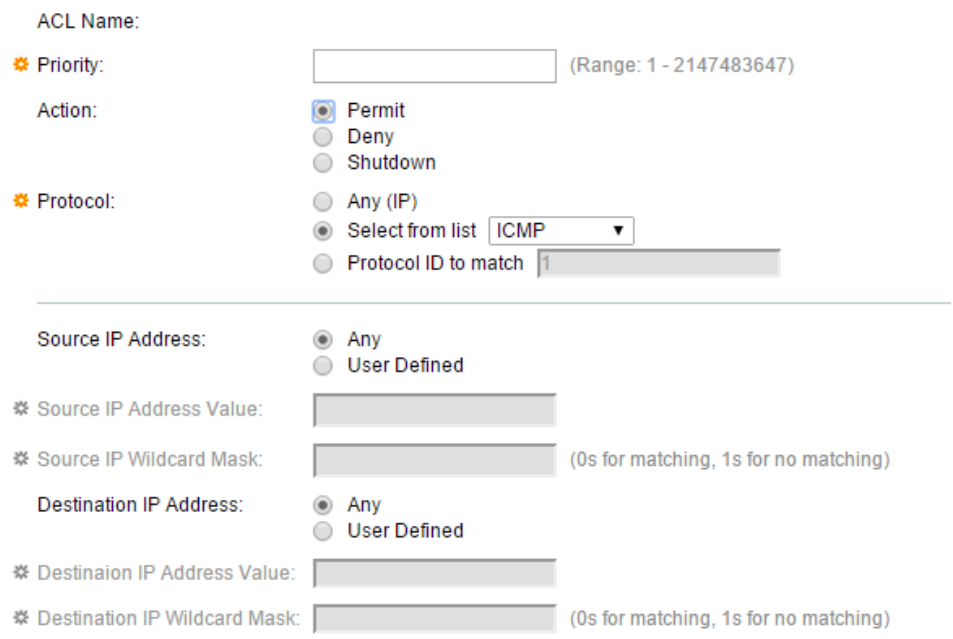
Nummer	**S14 - VLAN verspreiding**
Omschrijving test	Kan het apparaat VLANs distribueren?
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	VLANs aanmaken.
Toelichting	
Verwachte uitkomst	OK
Resultaat	NOK, SG200 heeft niet de optie om een VTP domain te maken of om hier lid van te worden
Datum test	14-11-2014
Maatregel	

Figuur 127 VLAN verspreiding – testgeval

Nummer	S15 - Security levels instellen
Omschrijving test	Bestaat er de mogelijkheid om gebruikers read only acces te geven| voor basis diagnostische taken
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	Verschillende users aanmaken op de switch met verschillende rechten.
Toelichting	
Verwachte uitkomst	OK
Resultaat	OK, Dit kan op de SG300 en er is keuze tussen readlonly, limited write en read/write (full)
	 Figuur 128 User account op SG300
Datum test	14-11-2014
Maatregel	

Figuur 129 Security levels - testgeval

Nummer	S16 - ACL's
Omschrijving test	Kan het apparaat VLANs distribueren?
Tester	Chris
Fase	PoC
Precondities	Beschikbaarheid apparaat
Handelingen	VLANs aanmaken.
Toelichting	
Verwachte uitkomst	OK
Resultaat	Ok, SG300 kan dit op zowel ipv4 als ipv6.
Datum test	14-11-2014
Maatregel	



Figuur 130 SG300 ACL

Figuur 131 ACL's - testgeval

5.3 TESTCASE: MALWARE BLOKKEREN

Deze testcase is tot stand gekomen nadat een aantal klanten geïnfecteerd zijn met een cryptolocker malware wat tot veel schade en dataverlies kan lijden. Cryptolocker malware zorgt ervoor dat bestanden op de pc van het slachtoffer met een zeer sterke encryptie worden versleuteld waarvan de gebruiker niet weet wat het wachtwoord is voor het ontsleutelen. Met andere woorden, de bestanden worden als het ware gegijzeld. Vervolgens verschijnen er links naar een website waar betaald kan worden om de sleutel voor ontgrendeling te verkrijgen.(Nachreinier, 2013)
Het doel is om te testen hoe de Watchguard firewall deze dreiging stopt via een vrije test. Dit alles wordt gedocumenteerd zodat Constant IT in de toekomst een soortgelijke instelling kan gebruiken bij klanten.

Voor deze test is een beveiligingsbundel geactiveerd welke toegang geeft tot de “best of breed” diensten van Watchguard, deze diensten zijn: (Watchguard, 2014)

Application control
Met deze optie vallen bepaalde applicaties te limiteren of blokkeren zoals games, p2p software en social media.

Gateway Antivirus
Dit is de eerste verdedigingslijn tegen virussen op de meest gebruikte protocollen. Er wordt geclaimd dat in combinatie met de APT blocker zelfs zero-day malware aanvallen gestopt kunnen worden.

Intrustion prevention service (IPS)
IPS scant verkeer op de meet gebruikte protocollen en beschermt tegen spyware, SQL injecties en buffer overflows. Nieuwe aanvallen kunnen snel herkend worden omdat er periodiek updates van Watchguard worden gedownload met de nieuwste “signatures”.

Reputation enabled defense
De handige features kan websites blokkeren op basis van ervaringen die andere Watchguard firewalls hebben gehad. Stel dat website mijnmalware.com door een groot aantal bedrijven is bezocht en daar telkens malware op werd aangetroffen. Dan zou deze website een zeer slechte reputatie hebben waardoor deze, wanneer dat ingesteld wordt, automatisch geblokkeerd zou kunnen worden. Deze feature bespaart resources voor de firewall omdat er minder gescand hoeft te worden.

Spamblocker
Blokkeert zoals de naam zegt spam, de spamblocker valt te koppelen aan de APT, IPS en gateway antivirus.

Webblocker
Met behulp van de webblocker kunnen websites of zelfs complete categorieën van websites geblokkeerd worden. Een voorbeeld is de categorie “social media” welke alle bekende social media sites blokkeert. Echter valt hier wel in te stellen dat bepaalde werknemers wel of niet binnen deze regels vallen zodat werknemers van de marketing afdeling toegang kunnen krijgen tot Facebook.

Data loss prevention (DLP)
Met DLP kan het al dan niet per ongeluk lekken van kritische bedrijfsinformatie zoals creditcardnummers worden tegen gehouden. Dit wordt gedaan door een reguliere expressie te maken. vervolgens wordt deze expressie in acht genomen bij uploads van bestanden of het sturen van mail. Wanneer de expressie gevonden wordt in een tekst wordt de mail of upload geblokkeerd of afgebroken.

Advanced persistent threat (APT)
APT probeert door te gaan waar de Gateway Antivirus stopt, dit houdt in dat APT bescherming biedt tegen malware waar nog geen signatures voor zijn. Volgens Lastline die deze dienst geïmplementeerd heeft in de Watchguard systemen kan 51% van de antivirusscanneer een mutatie of nieuwe vorm van malware niet herkennen op de 1ste dag dat deze op het internet rondzwerft. (Lastline, 2014)

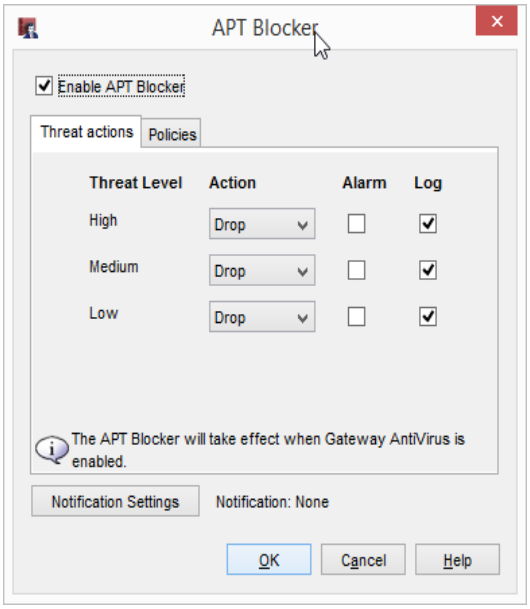
5.3.1 UITVOEREN TESTCASE

Voor de testcase is de originele infrastructuur zoals beschreven in het funtioneel ontwerp gewijzigd. Er wordt één Watchguard gebruikt met een verbinding naar het internet en één PC. Bij de training van Watchguard is geleerd dat geen enkel individueel systeem waterdicht is maar dat met een combinatie van allerlei systemen de meeste kans bestaat om malware buiten de deur te houden.
Voor de testcase worden een aantal Watchguard subscription services gebruikt namelijk:

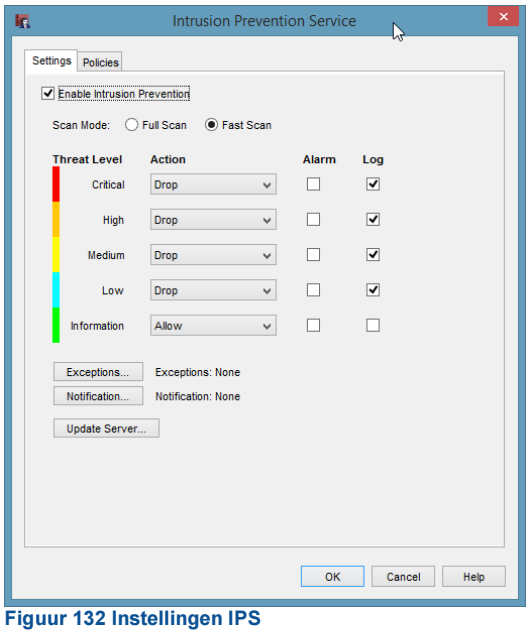
- IPS
- APT
- Reputation enabled defense
- Gateway antivirus

Door datapakketten door al deze diensten te laten filteren wordt volgens Watchguard een layered defense bereikt welke erg effectief is en zelfs zero-day malware kan detecteren.
Allereerst is er een trial geactiveerd voor de Watchguard services en zijn alle mogelijk te downloaden signatures geupdate naar de laatste versie.

Daarna zijn de verschillende services aangezet. De instellingen worden aangegeven in de figuren hieronder, uiteraard wordt alles gelogd zodat duidelijk is wat er gebeurd.



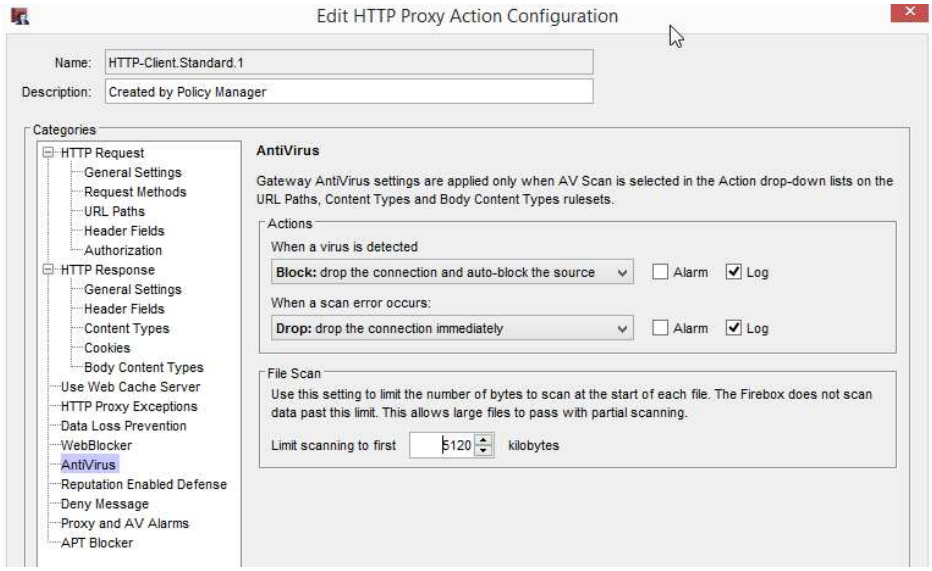
Figuur 133 Instellingen APT blocker



Figuur 132 Instellingen IPS

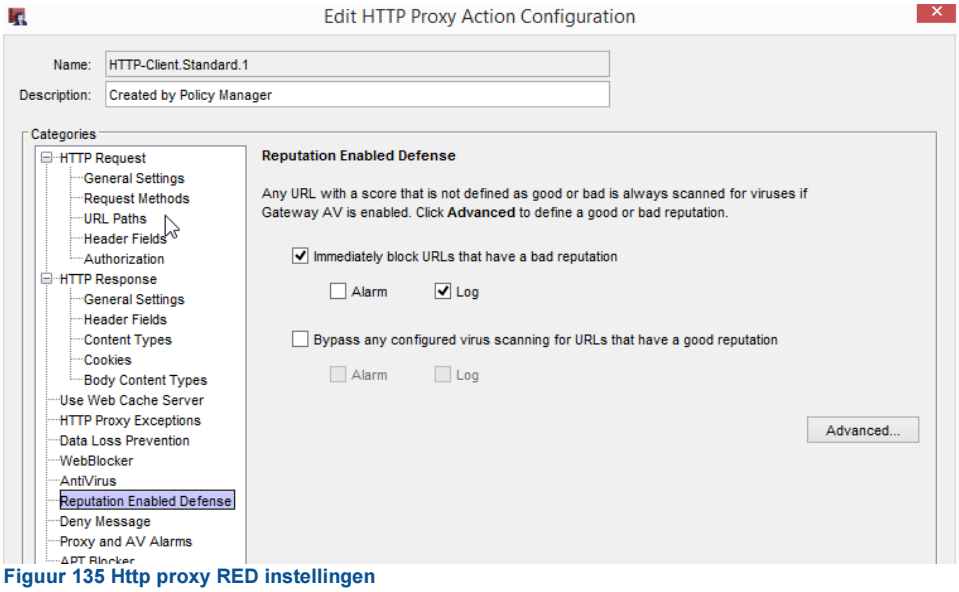
Voor de test wordt http en https verkeer gebruikt en wordt er (test)malware gedownload van het internet. Om internet verkeer te laten filteren door de Watchguard firewall moeten er proxy's worden aangemaakt, de instellingen zijn zoveel mogelijk standaard gelaten op een paar uitzonderingen na:

- Al het verkeer wordt door de Gateway Antivirus engine gehaald en pakketten worden geblockt wanneer een virus gedetecteerd wordt.
- Reputation enabled defense wordt geactiveerd op de http proxy zodat gebruikers niet naar websites kunnen waarvan bekend is dat die malware bevatten.
- De APT blocker die eerder is geactiveerd wordt aangezet zodat de proxy deze gebruikt. De APT blocker kan niet functioneren zonder Gateway Antivirus



Figuur 134 HTTP proxy Antivirus settings

De gateway antivirus is zo ingesteld dat als er scanfouten optreden door bijvoorbeeld het niet kunnen openen van een bestand (ZIP bestand met wachtwoord) dat deze direct gedropt wordt. De file scan limit wordt verhoogt tot 5MB zodat de scanneer het bestand verder door kijkt, de meeste virussen worden echter zo snel mogelijk in de code uitgevoerd. Daarnaast wordt alles gelogd zoals gesteld in best practices.

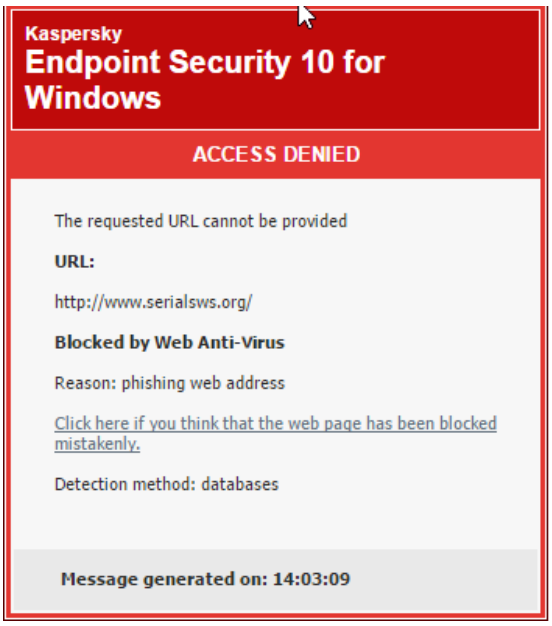


Figuur 135 Http proxy RED instellingen

Op de http proxy wordt ook de reputation enabled defense aangezet en gelogd. Op deze manier kan men zien wanneer een bepaalde gebruiker naar een als slecht aangeschreven site probeert te browsen
Er wordt niet gekozen om de instelling ”bypass any configured virus scanning for URL’s that have a good reputation” aan te vinken. Het is in het verleden wel eens voorgekomen dat bekende sites zoals Theguardian of NU.nl ineens (per ongeluk) malware bleken te hosten. Met deze optie zou deze malware vrij de ruimte hebben in het netwerk.

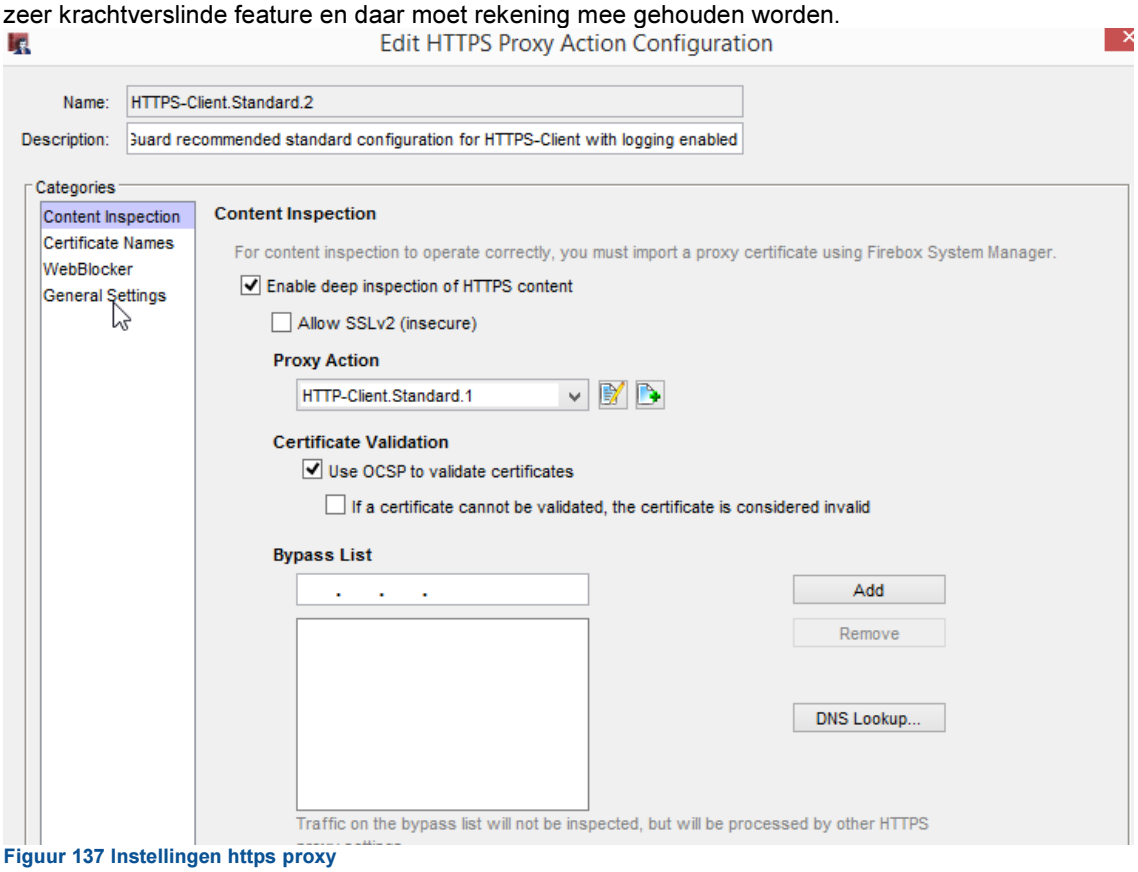
De reputatie is gebaseerd op een schaal van 1 tot 100, in de geavanceerde instellingen kan de beheerder zelf aangeven vanaf welke waarde een site als slecht wordt beschouwt. Als gebruiker een

website bezoekt met een slechte reputatie dan krijgt hij de onderstaande melding. Alle reputaties van de verschillende websites zijn te vinden op : http://www.borderware.com/index.php



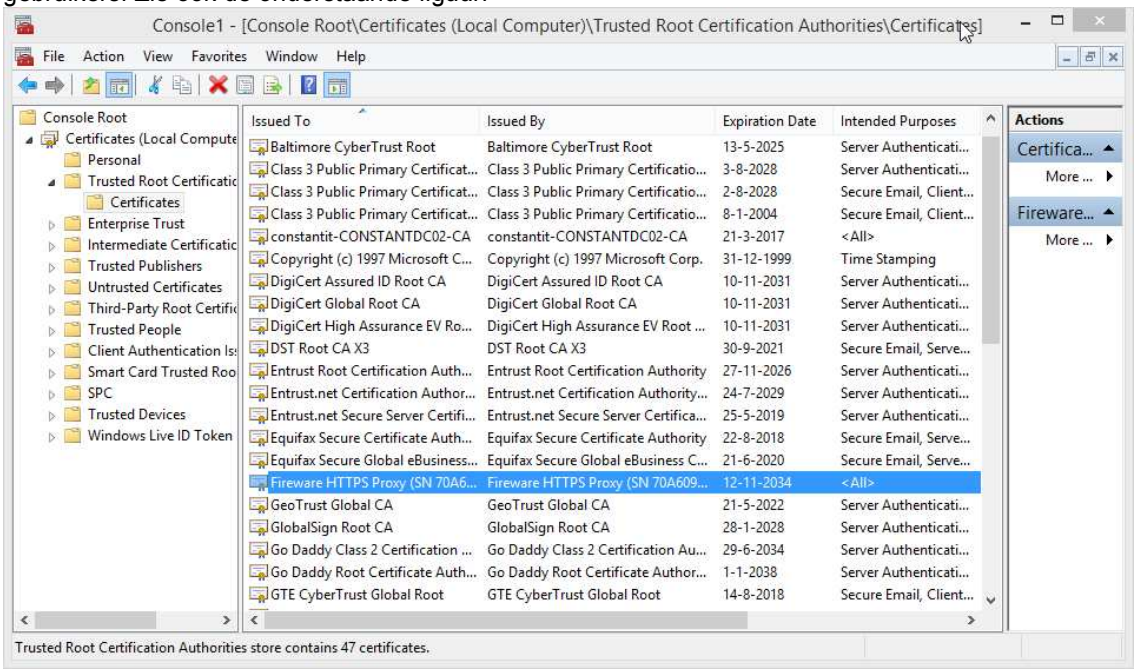
Figuur 136 Blokkeren website door RED

Nu de http proxy volledig ingesteld is kan er ook een https proxy gemaakt worden omdat verkeer ook via veilige verbindingen binnen kan komen. Binnen Watchguard is het instellen hiervan zo eenvoudig mogelijk gemaakt. In plaats van dat alle instellingen weer opnieuw ingesteld moeten worden kan er ook gekozen worden om dezelfde instellingen te gebruiken als de http proxy. Dit valt ook te zien in de onderstaand figuur. Daarnaast wordt “deep packet inspection” aangezet zodat ook dei inhoud gescand kan worden, dit is echter een zeer krachtverslinde feature en daar moet rekening mee gehouden worden.



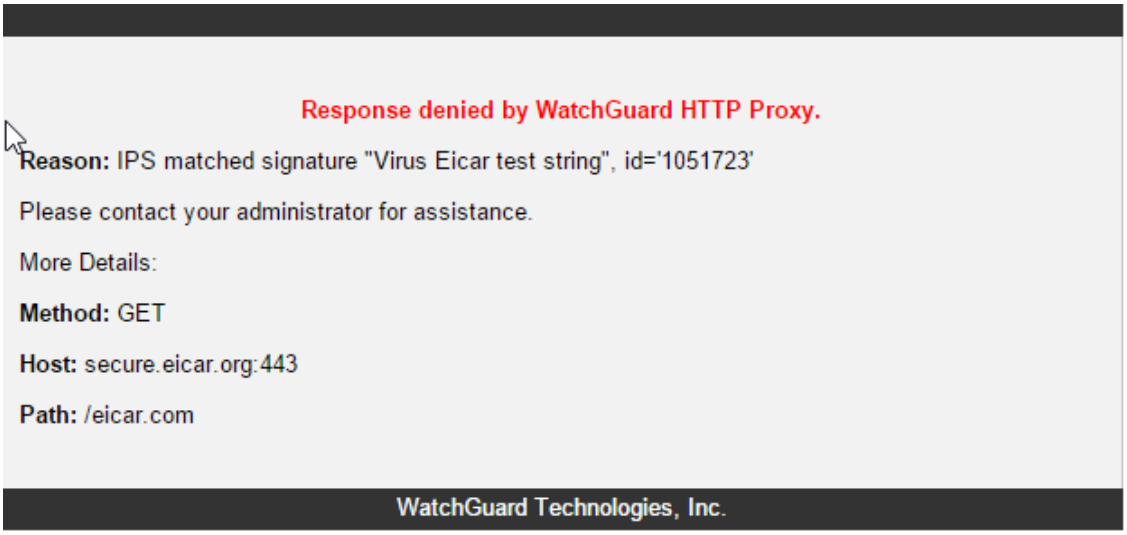
Figuur 137 Instellingen https proxy

Na het instellen krijgen alle websites een foutmelding omdat hen certificaat niet geldig is, dit wordt namelijk vervangen door het Watchguard certificaat bij het inspecteren. Hierom moet op de Watchguard het https proxy certificaat geëxporteerd worden en vervolgens geïmporteerd bij de gebruikers. Zie ook de onderstaande figuur.



Figuur 138 Trusted https certificaat Windows

Nu alles is ingesteld wordt er met behulp van een “Eicar malware test file[20]” geprobeerd om malware te downloaden en te draaien op de pc. Omdat dit om een welbekend testbestand gaat is voor deze test de antivirus op de lokale computer uitgeschakeld. Er wordt getest met behulp van de https proxy welke dezelfde instellingen gebruikt als de http proxy.
Het downloaden van het testbestand resulteert in de volgende melding:



Figuur 139 Blokkeren standaard malware testbestand via https

[20] http://www.eicar.org/85-0-Download.html

Het is vaak zo dat virussen in een zip bestand zitten of dat een virus in een zip bestand zit wat in een zip bestand zit. Op deze manier worden sommige virusscanners voor de gek gehouden. Er valt echter in te stelen hoe “diep” de scanner moet scannen. In de test is gekozen voor 3 niveaus. In de figuur hieronder wordt Eicar2.zip gedownload welke een zip archief bevat dat in een zip archief zit welke het malware testbestand bevat.

Figuur 140 Blokkeren dubbele zip eicar testbestand https

De Eicar testfiles worden tegen gehouden met behulp van de IPS en Gateway Antivirus oplossingen, dit wordt uiteraard ook weergegeven in de logs.

Figuur 141 Log van blokkeren dubbele zip eicar testbestand https

Echter zouden er ook nieuwe varianten kunnen ontstaan van oude malware of totaal nieuwe malware. Voor deze malware, de zogenoemde zero-day malware bestaan nog geen definities waardoor reguliere virusscanners geen herkenningspunt hebben. Dit is waar de APT blocker voor gebruikt wordt. De APT blocker probeert bestanden te scannen en verdacht gedrag te achterhalen, als er een verdacht bestand wordt gevonden wordt deze naar een in de cloud aanwezige “sandbox” omgeving gestuurd voor verdere analyse. Het bestand ongeacht of deze nu wel of niet gevaarlijk was wordt niet toegelaten in de netwerkomgeving en kan ook geen schade veroorzaken. Dit is echter de theorie en is niet in de praktijk getest.

6. CONCLUSIE

In het proof of concept zijn er veel verschillende tests gedaan en is er een testcase uitgevoerd. De resultaten hiervan laten zich het best zien in een numerieke waarde. In de tabel hieronder wordt aangegeven hoeveel testcases OK of NOK waren.

	Testcases met OK	Testcases met NOK	Totaal aantal testcases
SG200/SG300	14	2	16
Watchguard XTM26	21	0	21

Figuur 142 Overzicht succesvolle tests

Voor de firewall zijn alle tests met een OK afgerond wat betekend dat deze goed gebruikt kan blijven worden in omgevingen die Constant IT beheert. Voor de switches ligt dit wat lastiger, wij hadden beschikking tot een SG200 terwijl de SG300 was aanbevolen Gelukkig is er uiteindelijk de mogelijkheid geboden om een SG300 bij een klant te testen. Alle tests waarop de SG200 een OK zou kunnen scoren zijn op de SG200 uitgevoerd. De tests die niet uitgevoerd konden worden zijn uitgevoerd op de SG300, dit zijn de layer 3 tests zoals ACL's en het aanmaken van gebruikers met gelimiteerde toegang. De test hebben bewezen dat er 14 van de 16 tests met een OK beantwoord worden. Het gemis van de laatste twee features is geen probleem voor Constant IT omdat dit geen must have eisen waren. De twee geteste apparaten (Watchguard XTM26 en Cisco SG300 kunnen beiden succesvol ingezet worden in een klantomgeving).

De testcase wijst uit dat het met behulp van subscription services een zeer goede verdediging op valt te stellen met meerdere lagen. De verschillende scans, IPS, Gateway Antivirus, Reputation enabled defense en APT blocker werken goed samen en vallen eenvoudig in te stellen op de verschillende proxy's die aangemaakt zijn om verkeer te controleren. Door de malware testfiles van Eicar te gebruiken is gebleken dat dreigingen al gestopt worden voordat ze door bij wijze van spreken door de voordeur komen. Met de APT blocker is er ook een zekerheid tegen dreigingen die nog niet herkend worden door de andere scans. Het is dan ook aanbevolen om te proberen deze subscription services bij klanten aan te gaan bieden, met voldoende uitleg over de mogelijkheden en klanten bestaat de mogelijkheid dat klanten dit graag afnemen.

FIGURENLIJST

Figuur 83 Testopstelling PoC 7
Figuur 84 Testpunten firewall 9
Figuur 85 Testpunten switches 9
Figuur 86 Risicoclassificatie tabel 10
Figuur 87 Risicoclassficatie firewall 11
Figuur 88 Risicoclassficatie switches 11
Figuur 89 Multi WAN testgeval 13
Figuur 90 Gigabit poorten testgeval 13
Figuur 91 IPv6 testgeval 14
Figuur 92 Link aggregation testgeval 14
Figuur 93 Uitbreidbaarheid via licenties testgeval 14
Figuur 94 Loggen testgeval 15
Figuur 95 Reporting testgeval 15
Figuur 96 Site-to-site testgeval 16
Figuur 97 VPN troughput testcase 16
Figuur 98 VPN failover testgeval 17
Figuur 99 QoS testgeval 17
Figuur 100 DHCP testgeval 18
Figuur 101 NAT testgeval 18
Figuur 102 LDAP/AD testgeval 18
Figuur 103 IPsec testgeval 19
Figuur 104 VLAN testgeval 19
Figuur 105 ACL testgeval 20
Figuur 106 DDOS herkenning testgeval 22
Figuur 107 IDS/IPS testgeval 22
Figuur 108 Security levels testgeval 22
Figuur 109 Audit logs testgeval 23
Figuur 110 Ipv6 testgeval 24
Figuur 111 1Gbt testgeval 24
Figuur 112 Failover testgeval 24
Figuur 113 Stacking - testgeval 25
Figuur 114 Loggen testgeval 25
Figuur 115 Backup en export testgeval 25
Figuur 116 Remote access testgeval 26
Figuur 117 Console port - testgeval 26
Figuur 118 Diagnostische tools testgeval 26
Figuur 119 LACP instellingen 27
Figuur 120 Doorvoersnerlheid op laptop 28
Figuur 121 Etherchannel testgeval 28
Figuur 122 QoS opties 29
Figuur 123 QoS testgeval 29
Figuur 124 Statische route op SG300 29
Figuur 125 Layer 3 functionaliteit – testgeval 30
Figuur 126 Vlan testgeval 30
Figuur 127 VLAN verspreiding – testgeval 30
Figuur 128 User account op SG300 31
Figuur 129 Security levels - testgeval 31
Figuur 130 SG300 ACL 32
Figuur 131 ACL's - testgeval 32
Figuur 133 Instellingen IPS 34
Figuur 133 Instellingen APT blocker 34
Figuur 134 HTTP proxy Antivirus settings 35
Figuur 135 Http proxy RED instellingen 35
Figuur 137 Blokkeren website door RED 36
Figuur 137 Instellingen https proxy 36

Figuur 138 Trusted https certificaat Windows 37
Figuur 139 Blokkeren standaard malware testbestand via https 37
Figuur 140 Blokkeren dubbele zip eicar testbestand https 38
Figuur 141 Log van blokkeren dubbele zip eicar testbestand https 38
Figuur 142 Overzicht succesvolle tests 39

BRONNENLIJST

Alani, M. M. (2014). *Guide to OSI & TCP/IP Models.*

Cisco. (2005, Augustus 10). *Quality of service - Difference between policing and shaping.* Retrieved from Cisco: http://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html#policingvsshaping

Cisco.com. (2014). *Dropbox- SG300*. Retrieved from https://www.dropbox.com/s/2yz9nku2oqp1a5j/Sg300%20technical%20documentation.pdf?dl=0

Compare Business Products. (2014, 3 18). *Security: IDS vs. IPS Explained*. Retrieved from http://www.comparebusinessproducts.com/: http://www.comparebusinessproducts.com/fyi/ids-vs-ips

Horsten, C. (2012). *Tmap | Infrastructuur.* Vianen: Sogeti Nederland.

ING Nederland. (2013, 4 5). *Achtergronden storingen banken*. Retrieved from ING.nl: https://www.ing.nl/nieuws/nieuws_en_persberichten/2013/04/Achtergronden_storingen_banken.aspx?first_visit=true

International Institute of Buisiness Analysis. (2009). *a guide to the business analysis body of knowledge (babok guide)* . Retrieved from http://www.iowadnr.gov/: http://www.iowadnr.gov/portals/idnr/uploads/Iowa%20Outdoors%20News/2011/BABOK%20Version2.pdf

Lastline, G. V. (2014, 5 21). *Antivirus Isn't Dead, It Just Can't Keep Up*. Retrieved from Labs.lastline.com: http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up

Microsoft . (2003, 03 28). *What Is IPSec?* Retrieved from Microsoft Technet: http://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx

Nachreinier, C. (2013). *Everything you wanted to knkow about cryptolocker*. Retrieved from Watchguardsecuitycenter.com: http://Watchguardsecuritycenter.com/2013/11/04/everything-you-wanted-to-know-about-cryptolocker/

Paul Congdon, I. (02, 7 3). *Link Layer Discovery*. Retrieved from http://www.ieee802.org/: http://www.ieee802.org/1/files/public/docs2002/lldp-protocol-00.pdf

Rajesh, K. (2012, May 25). *What is LLDP (Link Layer Discovery Protocol)?* Retrieved from exclTingIP.com: http://www.excitingip.com/3026/what-is-lldp-link-layer-discovery-protocol/

RIPE NCC. (2014, 6 24). *Reaching the last /8*. Retrieved from www.ripe.net: http://www.ripe.net/internet-coordination/ipv4-exhaustion/reaching-the-last-8

Schellevis, J. (2012, 9 14). *RIPE NCC deelt laatste blok ipv4-adressen uit*. Retrieved from Tweakers: http://tweakers.net/nieuws/84386/ripe-ncc-deelt-laatste-blok-ipv4-adressen-uit.html

StarTrinity. (2014). *Startrinity network tester*. Retrieved from Startrinity.com: http://startrinity.com/VoIP/NetworkTester/NetworkTester.aspx

Steehouder, M. (2012). *Leren Comminuceren.* Noordhoff Uitgevers B.V.

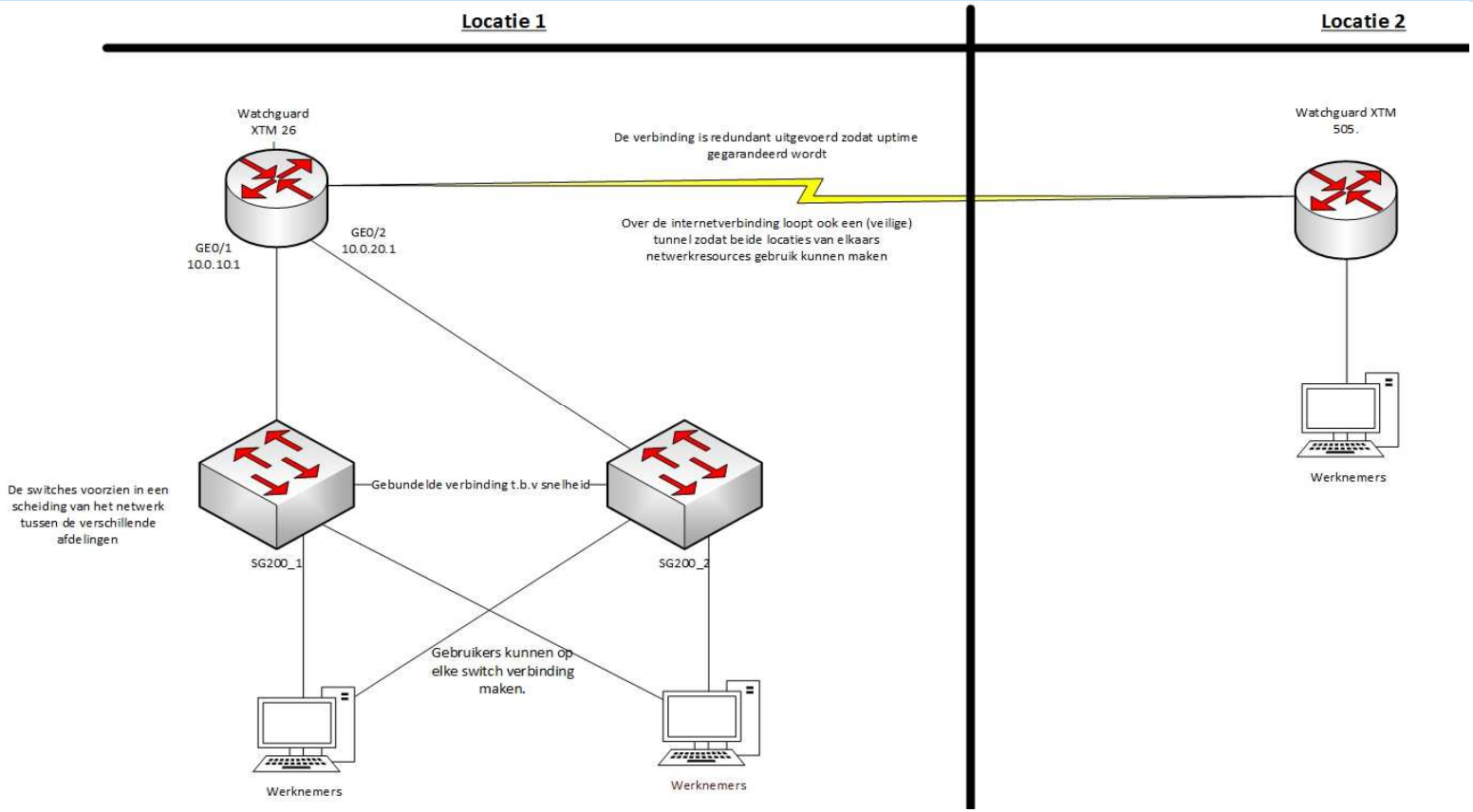
TOGAF. (2011). *Togaf 9.1 overview*. Retrieved from togaf.com: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap37.html

Watchguard. (2014). *Dropbox - Watchguard fireware essentials*. Retrieved from https://www.dropbox.com/s/2yz9nku2oqp1a5j/Sg300%20technical%20documentation.pdf?dl=0

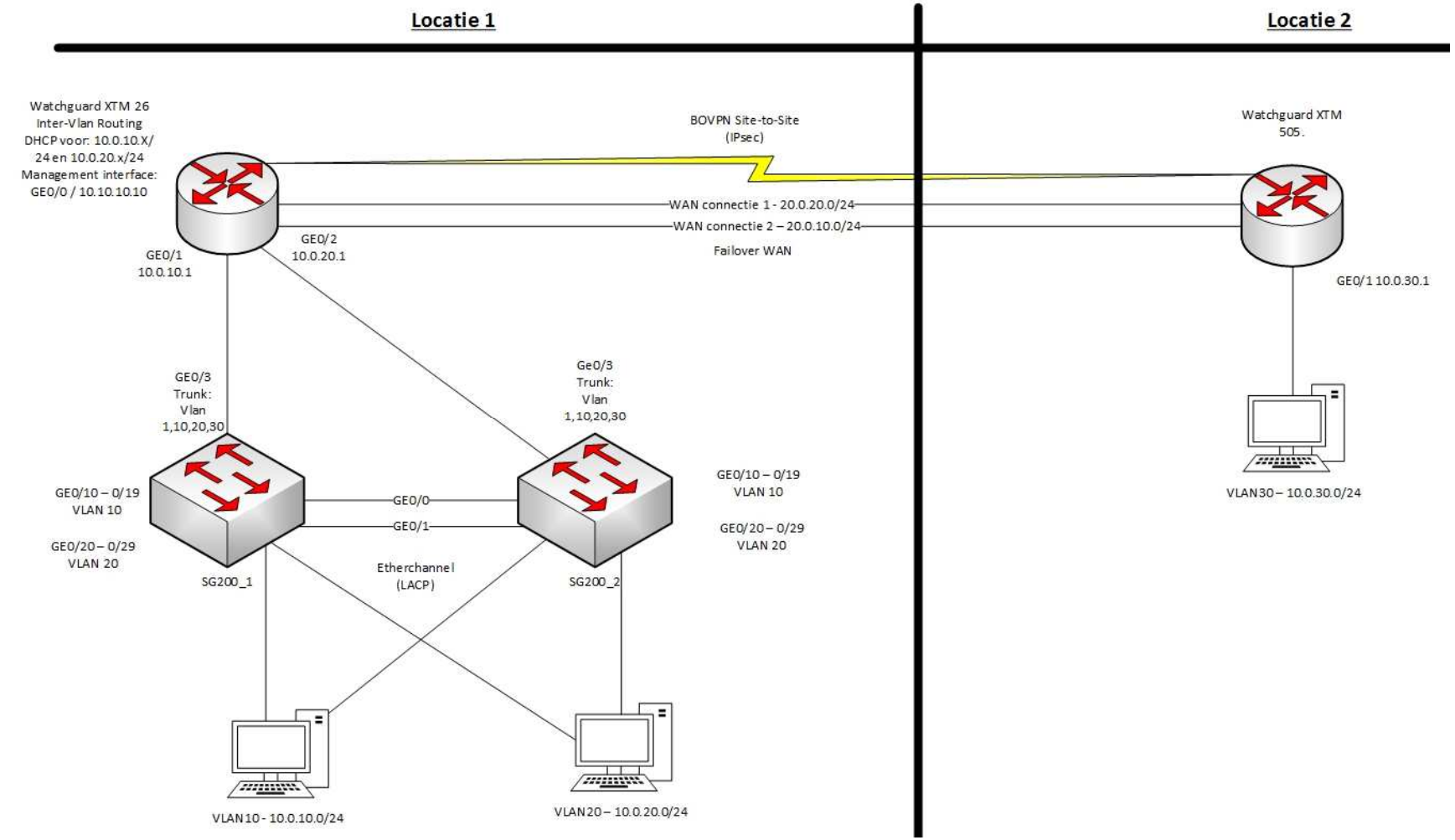
Watchguard. (2014). *UTM security modules*. Retrieved from http://Watchguard.com/wgrd-products/utm/overview/#utm-security-modules

BIJLAGE

BIJLAGE 1 FUNCTIONEEL ONTWERP



BIJLAGE 2 TECHNISCH ONTWERP



Building blocks

Constant IT
16 december 2014, Chris de Keijzer

Auteur: Chris de Keijzer
Opleiding: System & Network engineering
Studentnummer: 1591134
Telefoonnummer: 06-10181296
Datum: 9-12-2014
Versie: 1.0

Documentinformatie
Documentbeheer en Goedkeuring

Versie	Auteur	Opmerkingen	Document Eigenaar	Datum
1.0	Chris de Keijzer	Eerste versie	Chris de Keijzer	4-12-2014

Dit document is beoordeeld door

Versie	Naam	Functie	Datum beoordeling

Dit document is goedgekeurd door

Versie	Naam	Functie	Datum beoordeling
1.0			

INHOUDSOPGAVE

1 Inleiding 48
2 Building block 49
2.1 Wat is een building block? 49
3 De building blocks van COnstant IT 49
3.1 Building BLOCK P1 “Klein zakelijk” 50
3.1.1 Netgear LGS124 50
3.1.2 Draytek 2130 50
3.2 Building BLOCK p2 “MKB” 52
3.2.1 Cisco SG300 53
3.2.2 Watchguard XTM 26 53
3.3 Building BLOCK p3 “MKB+” 56
3.3.1 Cisco SG500 57
3.3.2 Watchguard XTM3 series 57
4 Conclusie 59

1. INLEIDING

Dit document is het resultaat van het vergelijkend onderzoek en proof of concept dat gedaan is bij Constant IT. De building blocks bestaat uit een apparaat en een daarbij horende standaardconfiguratie. Dit document is toelichting op de building blocks tekening die gemaakt is en zal de meest belangrijke zaken uitleggen. Dit document is bedoeld voor de verschillende technische specialisten van Constant IT welke hiermee een aantal basisacties kunnen uitvoeren op de best getest apparatuur. Daarnaast functioneert het document ook als bijlage op de building blocks die gemaakt zijn. In hoofdstuk 2 wordt gestart met een uitleg van wat een building block precies is. In hoofdstuk 3 wordt uitgelegd wat de building blocks van Constant IT zijn en hoofdstuk 4 bevat een conclusie.

2. BUILDING BLOCK

Dit hoofdstuk bevat informatie over wat een building block precies is en hoe deze binnen Constant IT gebruikt zou kunnen worden.

2.1 WAT IS EEN BUILDING BLOCK?

Een building block is een herbruikbaar stuk business, IT of andere architectuur welke met andere building blocks gekoppeld kan worden om oplossingen te leveren. Volgens de TOGAF methode is men bij een building block vrij om een detail te definiëren. Zodoende zouden er high-level building blocks gemaakt kunnen worden maar ook building blocks die zeer gedetailleerd zijn(low level). Het niveau waarmee gedetailleerd dient te worden is sterk afhankelijk van de wens die vervuld behoord te worden. (TOGAF, 2011)
Een building block heeft een aantal karakteristieken, de voor Constant IT meest relevante zijn:

Een building block is een pakket aan functionaliteit dat in een bepaalde wens voorziet;
Een building block heeft een duidelijke grens of afbakening;
Een building block kan samenwerken met andere buiding blocks;
Een building block is herbruikbaar, vervangbaar en goed gedocumenteerd.

3. DE BUILDING BLOCKS VAN CONSTANT IT

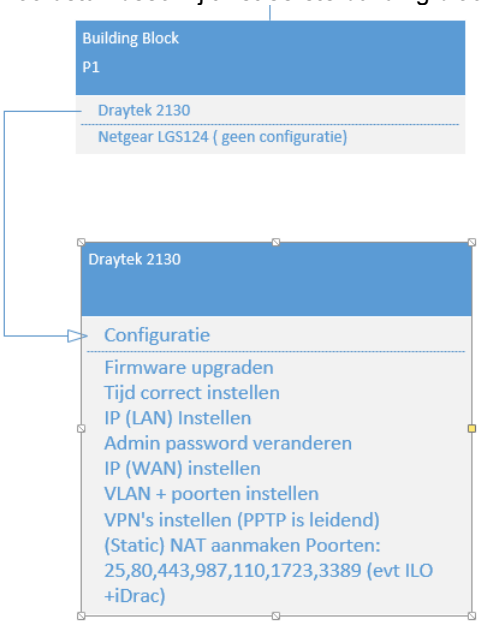
Het project dat nu gedaan wordt betreft het standaardiseren van apparatuur. Echter is standaardiseren meer dan slechts een productvergelijking welke een aantal producten oplevert. Hierom is er voor Constant IT een aantal building blocks gemaakt. Dit zijn low-level building blocks en geven aan welk apparaat + configuratie op een apparaat staat. Uiteraard kunnen configuraties waar nodig anders zijn omdat elke klant immers andere wensen heeft maar er dient zoveel mogelijk aan de gestelde basis configuratie gehouden te worden.

Er is eerder al gekozen voor een aantal categorieën, hierop zijn de building blocks gebaseerd.
P1 “Klein zakelijk”
P2 “MKB”
P3 “MKB +”

In de hoofdstukken hieronder worden de building blocks tekstueel behandeld ter aanvullen op de tekening die gemaakt is. De standaard configuratie wordt per building block beschreven. Het doel is om de configuraties over de klanten zo gelijk te maken als mogelijk is, uiteraard zullen er altijd kleine verschillen blijven.

3.1 BUILDING BLOCK P1 “KLEIN ZAKELIJK”

Dit hoofdstuk beschrijft het eerste building block welke voor de kleinste klanten van toepassing is.



Figuur 143 Building block P1

3.1.1. NETGEAR LGS124

Eerste poort is de verbinding naar het volgende netwerk apparaat, dit kan een switch of een router zijn. Verder is er geen configuratie mogelijk gezien dit een unmanaged switch betreft.

3.1.2 DRAYTEK 2130

1. Firmware updaten

System maintenance --> firmware upgrade
Upgrade de firmware als eerst, altijd de nieuwste (non-beta) versie. Gebruik de "web firmware upgrade optie en verwijs naar een bestand op de PC welke vooraf gedownload is.

2. Tijd instellen

System maintenance --> time and date
Deze kan geïmporteerd worden vanaf de lokale PC

3. LAN IP instellen

System maintenance --> management -> IPv4 management setup
Stel hier de instellingen van het LAN in, de draytek is altijd te benaderen vanaf het LAN netwerk en is tenzij expliciet anders vermeld het eerste IP op het (sub) netwerk.

4. WAN IP instellen

WAN--> WAN setup
De juiste instellingen worden aangeleverd door SD.

5. VLAN Configuratie

LAN--> VLAN
Vul eventuele VLAN configuratie in en geef aan op welke poort deze behoren te staan.
VLAN 10 = data
VLAN 20 = gasten

6. Password veranderen

System maintenance --> administrator Password
User = admin + standaard password CIT

7. VPN's aanmaken (maximaal 2 op dit apparaat)

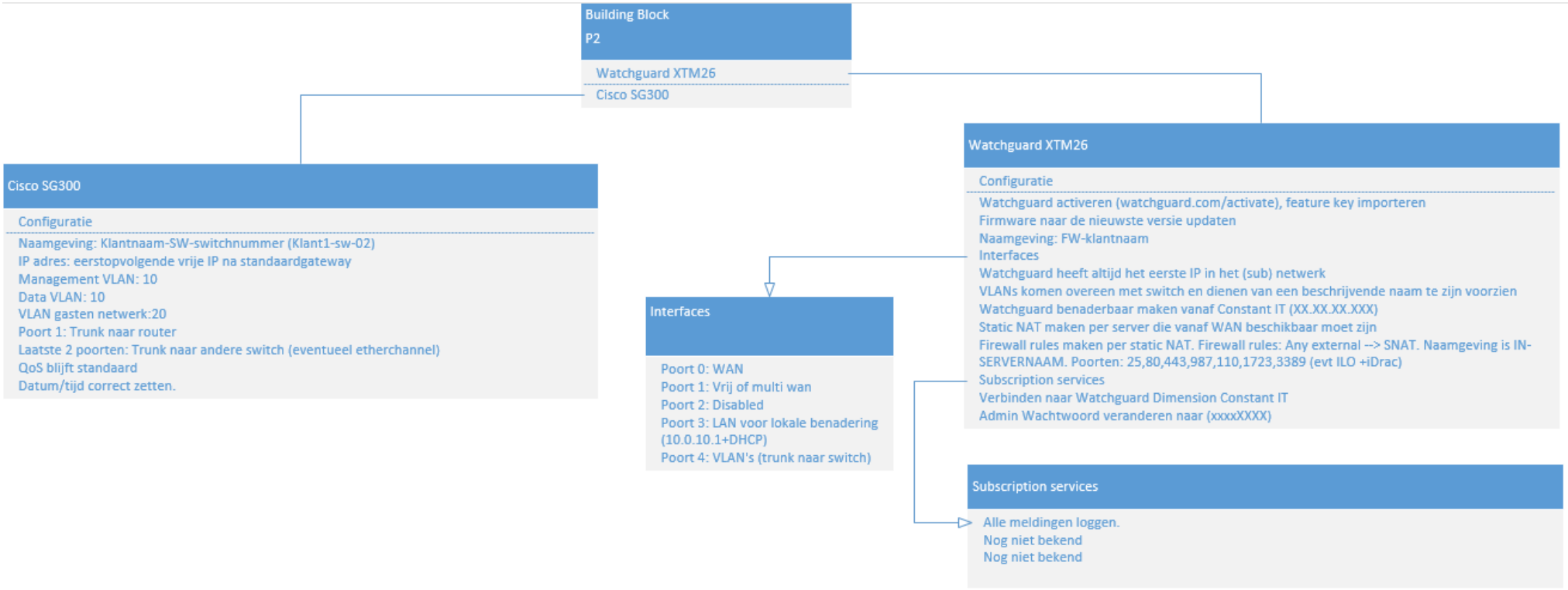
VPN--> Remote access
Maak eventueel VPNs aan, standaard is het PPTP protocol. De gegevens worden aangeleverd door SD.

8. Toegang servers vanaf WAN

NAT --> open ports
Voer hier in welke poorten bereikbaar moeten zijn vanaf het WAN netwerk, voorzie deze van een duidelijke naam. De informatie wordt aangeleverd door SD

3.2 BUILDING BLOCK P2 “MKB”

In de figuur hieronder eerst een overzicht van het volledige P2 building block, in de tekst hieronder wordt per instelling uitgelegd hoe deze bereikt kan worden



Figuur 144 Building block P2

3.2.1 CISCO SG300

1. Firmware updaten

Getting started → upgrade device software
Allereerst dient de firmware geüpdatet te worden naar (1.4.0.88) . Vergeet niet de “active image” aan te passen nadat dit klaar is.

2. Naamgeving veranderen

Administration → System settings
Pas de hostname aan naar: klantnaam-sw0X. De X wijst naar het nummer van de switch. Plak een sticker op de switch met dezelfde naam.

3. VLANs aanmaken

Vlan management → create VLAN
Onderstaande instellingen gelden altijd tenzij expliciet anders vermeld
VLAN 10 = data
VLAN 20 = gasten

4. VLANs toewijzen aan poorten

Vlan management → port to vlan
Gebruik de lijst met poorten welke door SD is aangereikt en stel dat in zoals opgeschreven.

5. Management VLAN aanpassen

VLAN management → default VLAN settings
VLAN 10 is ook het management VLAN.

6. IP adres veranderen

IP configuration → management and IP interfaces →IPv4 interface
Selecteer Add, de switch heeft altijd het eerstvolgende vrije IP na de standaardgateway (Watchguard)

7. Trunks aanmaken naar router en switch

VLAN management → Interface Settings
Poort 1 is altijd de trunk naar de router, de laatste twee poorten zijn altijd voor trunk naar andere switches.
Poort staan standaard op Trunk en laten alle VLANs controleer dat de juiste poorten zijn getrunked.

8. Datum/tijd correct zetten

Administration → time settings → system time
Vink Main Clock Source aan.
Ga naar SNTP settings en selecteer add. Voeg de timeserver toe

```
server 0.nl.pool.ntp.org
server 1.nl.pool.ntp.org
server 2.nl.pool.ntp.org
server 3.nl.pool.ntp.org
```

3.2.1 WATCHGUARD XTM 26

Er wordt bij deze configuratie gebruik gemaakt van de webinterface.

1. Watchguard activeren

De serial key op het apparaat dient ingevoerd te worden op www.Watchguard.com/activate. Van daaruit kan ook de feature key gekopieerd worden welke essentieel is voor de werking van de Watchguard. Via system → feature key kan de feature key geïmporteerd worden.

2. Firmware updaten

System → upgrade OS

De system software kan hier geüpdatet worden nadat deze gedownload is van de Watchguard website. Het is het makkelijkst om via de eigen laptop de update te draaien, hiervoor zijn bestanden nodig met het woord “SYSA-DL” erin.
Op het moment van schrijven is 11.9 de laatste versie en deze dient geïnstalleerd te worden

3. Naam aanpassen

System → information
Vul ook locatie en contact gegevens in

4. Interfaces aansluiten

De interfaces op de Watchguard dienen altijd als volgt ingedeeld en gelabeld te worden. De eerste 2 poorten zijn altijd WAN en de laatste altijd (V)LAN van de klant
Poort 0 : WAN
Poort 1: Vrij of multi-Wan
Poort 2:Disabled
Poort 3: LAN voor lokale benadering door Constant IT
Poort 4: (V)LAN naar lokale netwerk klant.

5. IP instellen (LAN/WAN)

Network → interfaces
Per interface een IP geven, interfaces zijn:
Internal (LAN). Het IP aan deze interface is altijd het eerste IP in het (sub) netwerk
VLAN: Deze interfaces werken hetzelfde als LAN maar wordt met een trunk verbinding naar het LAN verbonden.
Extrernal (WAN). De gegevens van de WAN verbinding worden altijd aangereikt door SD
Disabled.

6. VLANs aanmaken (gelijk aan switch)

VLAN’s moeten atijd gelijk zijn aan de VLANs op de switches.
VLAN 10 = data
VLAN 20 = gasten

7. Watchguard benaderbaar maken vanaf Constant IT

Firewall→ firewall policies
Wijzig de policy “Watchguard Web UI” zodat deze het externe ip van Constant IT doorlaat (xx.xx.xx.xxx)

8. Static NAT aanmaken

Firewall → SNAT
Voor elke server die vanaf het WAN benaderbaar dient te worden moet een static NAT entry gemaakt worden. De naam van de SNAT entry is altijd de servernaam naar waar deze verwijst. De poortenljist wordt opgeleverd door SD.

9. Firewall regels maken voor static NAT

Firewall → firewall policies
De statische NAT entries moeten ook door de firewall kunnen, hiervoor moeten firewall regels aangemaakt worden
Any external --> SNATNAAM.
Naamgeving van de regels is altijd :Directie-Taak , een voorbeeld is IN-SERVERNAAM of OUT-TELNET .

10. VPN’s aanmaken

VPN – Branch Office VPN
Er dienen eerste gateways gemaakt te worden, dit is het adres welke het eindpunt van de tunnel is. In het geval van een multi wan configuratie kunnen er meerdere gateways aangemaakt worden naar het zelfde adres.

Daarna kan er bij tunnels op “add” geklikt worden. Een tunnel gaat altijd over een gateway en kan ook gebruik maken van meerdere gateways.

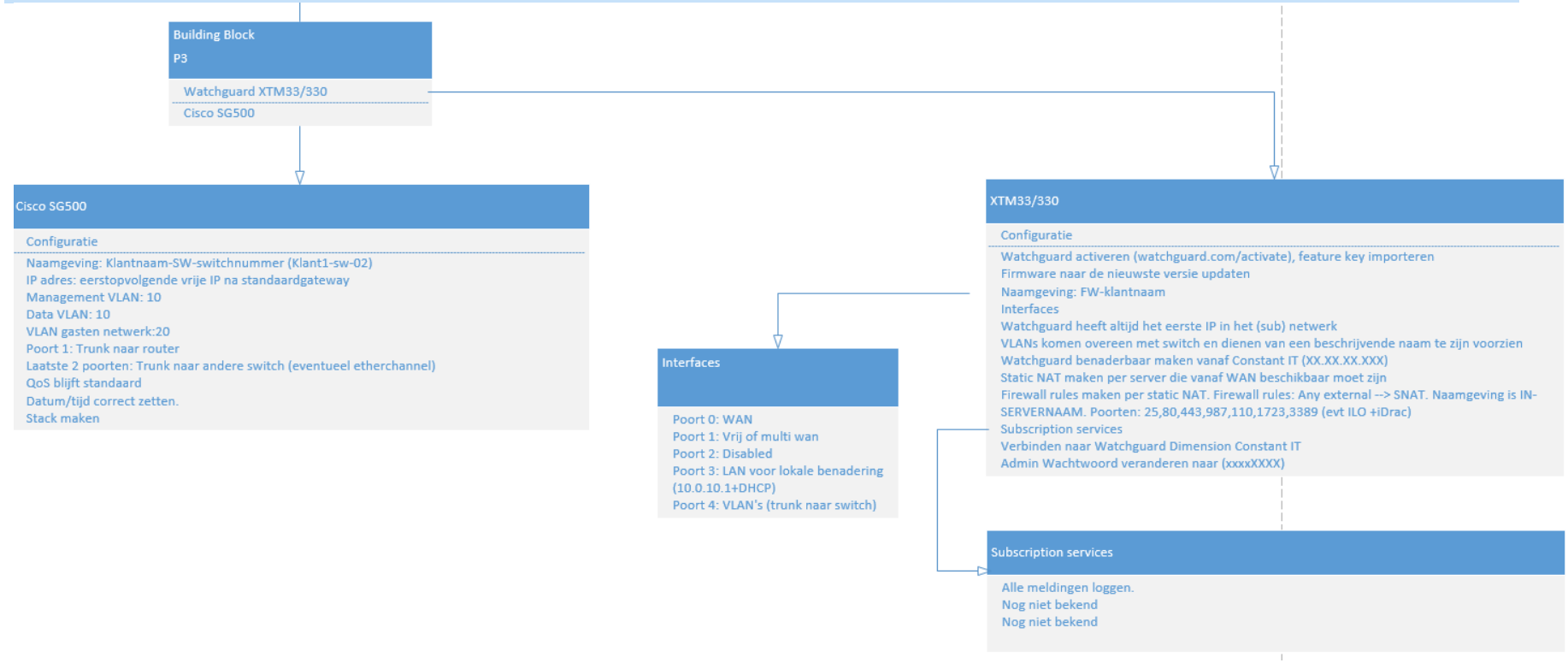
11. Verbinding naar Watchguard Dimension Service

System → logging
Selecteer ADD en verwijs naar het constant IT IP (xx.xx.xx.xxx) met als encryption key: logencrypt.

12. Admin wachtwoord veranderen

System → users and roles
Selecteer het admin account en wijzig het wachtwoord naar het standaard Constant IT wachtwoord (xxxxXXXX)

3.3 BUILDING BLOCK P3 “MKB+”



Figuur 145 Building block P3

3.3.1 CISCO SG500

1. Firmware updaten

Getting started → upgrade device software
Allereerst dient de firmware geüpdatet te worden naar (1.4.0.88) . Vergeet niet de “active image” aan te passen nadat dit klaar is.

2. Naamgeving veranderen

Administration → System settings
Pas de hostname aan naar: klantnaam-sw0X. De X wijst naar het nummer van de switch. Plak een sticker op de switch met dezelfde naam.

3. VLANs aanmaken

Vlan management → create VLAN
Onderstaande instellingen gelden altijd tenzij expliciet anders vermeld
VLAN 10 = data
VLAN 20 = gasten

4. VLANs toewijzen aan poorten

Vlan management → port to vlan
Gebruik de lijst met poorten welke door SD is aangereikt en stel dat in zoals opgeschreven.

5. Management VLAN aanpassen

VLAN management → default VLAN settings
VLAN 10 is ook het management VLAN.

6. IP adres veranderen

IP configuration → management and IP interfaces →IPv4 interface
Selecteer Add, de switch heeft altijd het eerstvolgende vrije IP na de standaardgateway (Watchguard)

7. Trunks aanmaken naar router en switch

VLAN management → Interface Settings
Poort 1 is altijd de trunk naar de router, de laatste twee poorten zijn altijd voor trunk naar andere switches.
Poort staan standaard op trunk en laten alle VLANs controleer dat de juiste poorten zijn getrunked.

8. Datum/tijd correct zetten

Administration → time settings → system time
Vink Main Clock Source aan.
Ga naar SNTP settings en selecteer add. Voeg de timeserver toe

```
server 0.nl.pool.ntp.org
server 1.nl.pool.ntp.org
server 2.nl.pool.ntp.org
server 3.nl.pool.ntp.org
```

9. Stacking instellen

Getting started → system mode and stack management
De eerste switch in de reeks is altijd de “stack master”. Verder is dit afhankelijk van info verschaft door SD is het een L2 of L3 stack omdat niet elke klant stacking zal gebruiken.

3.3.2 WATCHGUARD XTM3 SERIES

Deze gebruikt dezelfde basis configuratie als de XTM26
Er wordt bij deze configuratie gebruik gemaakt van de webinterface.

1. Watchguard activeren

De serial key op het apparaat dient ingevoerd te worden op www.Watchguard.com/activate. Van daaruit kan ook de feature key gekopieerd worden welke essentieel is voor de werking van de Watchguard. Via system → feature key kan de feature key geïmporteerd worden.

2. Firmware updaten

System → upgrade OS
De system software kan hier geüpdatet worden nadat deze gedownload is van de Watchguard website. Het is het makkelijkst om via de eigen laptop de update te draaien, hiervoor zijn bestanden nodig met het woord “SYSA-DL” erin.
Op het moment van schrijven is 11.9 de laatste versie en deze dient geïnstalleerd te worden

3. Naam aanpassen

System → information
Vul ook locatie en contact gegevens in

4. Interfaces aansluiten

De interfaces op de Watchguard dienen altijd als volgt ingedeeld en gelabeld te worden. De eerste 2 poorten zijn altijd WAN en de laatste altijd (V)LAN van de klant
Poort 0 : WAN
Poort 1: Vrij of multi-Wan
Poort 2:Disabled
Poort 3: LAN voor lokale benadering door Constant IT
Poort 4: (V)LAN naar lokale netwerk klant.

5. IP instellen (LAN/WAN)

Network → interfaces
Per interface een IP geven, interfaces zijn:
Internal (LAN). Het IP aan deze interface is altijd het eerste IP in het (sub) netwerk
VLAN: Deze interfaces werken hetzelfde als LAN maar wordt met een trunk verbinding naar het LAN verbonden.
Extrernal (WAN). De gegevens van de WAN verbinding worden altijd aangereikt door SD
Disabled.

6. VLANs aanmaken (gelijk aan switch)

VLAN’s moeten atijd gelijk zijn aan de VLANs op de switches.
VLAN 10 = data
VLAN 20 = gasten

7. Watchguard benaderbaar maken vanaf Constant IT

Firewall→ firewall policies
Wijzig de policy “Watchguard Web UI” zodat deze het externe ip van Constant IT doorlaat (xx.xx.xx.xxx)

8. Static NAT aanmaken

Firewall → SNAT
Voor elke server die vanaf het WAN benaderbaar dient te worden moet een static NAT entry gemaakt worden. De naam van de SNAT entry is altijd de servernaam naar waar deze verwijst. De poortenljist wordt opgeleverd door SD.

9. Firewall regels maken voor static NAT

Firewall → firewall policies
De statische NAT entries moeten ook door de firewall kunnen, hiervoor moeten firewall regels aangemaakt worden
Any external --> SNATNAAM.

Naamgeving van de regels is altijd :Directie-Taak , een voorbeeld is IN-SERVERNAAM of OUT-TELNET .

10. VPN's aanmaken

VPN – Branch Office VPN
Er dienen eerste gateways gemaakt te worden, dit is het adres welke het eindpunt van de tunnel is. In het geval van een multi wan configuratie kunnen er meerdere gateways aangemaakt worden naar het zelfde adres.

Daarna kan er bij tunnels op "add" geklikt worden. Een tunnel gaat altijd over een gateway en kan ook gebruik maken van meerdere gateways.

11. Verbinding naar Watchguard Dimension Service

System → logging
Selecteer ADD en verwijs naar het constant IT IP (xx.xx.xx.xxx) met als encryption key : logencrypt.

12. Admin wachtwoord veranderen

System → users and roles
Selecteer het admin account en wijzig het wachtwoord naar het standaard Constant IT wachtwoord (xxxxXXXX)

4. CONCLUSIE

Met behulp van de building blocks is er van de apparaten welke als meest geschikt uit de productvergelijking kwamen en standaardconfiguratie gemaakt. Deze standaardconfiguratie zorgt ervoor dat op langere termijn alle klantconfiguraties vrijwel gelijk zijn. Daarnaast is het zo dat door het beschrijven van de configuratie het document ook gebruikt kan worden als naslagwerk. Uiteindelijk zorgt dit ervoor dat alle medewerkers binnen Constant IT basistaken kunnen uitvoer op de netwerkapparatuur waardoor niet al het werk op deze apparaten bij enkele personen ligt.