PinkRoccade Healthcare bv
Fauststraat 3 | 7323 BA Apeldoorn
Postbus 20054 | 7302 HB Apeldoorn

T 055 599 92 00
F 055 599 92 01
SERVICE CENTER 0800 9119
W www.pinkroccade-healthcare.nl
E prhc.SecrApeldoorn@pinkroccade.nl

Data Center Netwerk Design

Redesign PRHC Data Center netwerk

DATUM	2 april 2013
PLAATS	Apeldoorn
AUTEUR	Wim de Ruijter (Network Consultant- HP)
	Eddie Vels (Technisch Specialist – PinkRoccade Healthcare)
CLASSIFICATIE	Strikt vertrouwelijk
VERSIE	1.02

Documentbeheer				
Versie	**Status**	**Auteur**	**Datum**	**Opmerking**
1.02	Final	EVE	02-04-2013	Final Document

Distributielijst		
Naam	**Organisatie / Afdeling**	**Datum**

Inhoudsopgave

1. Management summary

Door extreme groei van het PinkRoccade Healthcare datacenter over de afgelopen jaren is de noodzaak ontstaan om het huidige netwerk design te herzien en op te schalen om groei van de komende jaren op te vangen. De meest belangrijke speerpunten binnen dit nieuwe design zijn verbeterde betrouwbaarheid van de infrastructuur, betere informatiebeveiliging en vereenvoudigd beheer van de omgeving. Verder is van belang dat de nieuwe omgeving schaalbaar is maar ook fysiek kan worden geplaatst in de data center kasten zoals die nu in gebruik zijn in de data centers in Aalsmeer en Haarlem.

Er is een design uitgewerkt op basis van het Adaptive Networking Architecture concept waarbij een centrale backbone, de Transit core, de verschillende deelnetwerken koppelt. Beveiliging wordt geimplementeerd op het koppelpunt. De bestaande legacy omgeving wordt opgeknipt en gekoppeld aan de Transit core en een nieuwe klantomgeving wordt opgebouwd op de Edge core.

Er is gekozen voor losse componenten (fixed port switches georganiseerd in switch stacks en firewall appliances) die flexibel in de beschikbare kastruimte passen.

2. Inleiding

PinkRoccade Healthcare (PRH) biedt gespecialiseerde IT-oplossingen en diensten aan ziekenhuizen, gezondheidscentra, medische klinieken en andere zorgorganisaties in Nederland.

Veel van deze diensten worden gehost vanuit het PinkRoccade Healthcare datacenter, het ZCC (Zorg Computer Centrum).

Door extreme groei van het PinkRoccade Healthcare datacenter over de afgelopen jaren is de noodzaak ontstaan om het huidige netwerk design te herzien en op te schalen om groei van de komende jaren op te vangen. De meest belangrijke speerpunten binnen dit nieuwe design zijn verbeterde betrouwbaarheid van de infrastructuur, beter informatie beveiliging en vereenvoudigd beheer van de omgeving.

In de volgende hoofdstukken wordt een vernieuwd ontwerp voor het PRH data center besproken gericht op het behalen van bovenstaande doelen. Hoofdstuk 3 geeft een kort overzicht van de bestaande situatie. Hoofdstuk 4 geeft de requirements voor het design. Hoofdstuk 5 presenteert het nieuwe design en hoofdstuk 6 tenslotte geeft in grote lijnen aan hoe het bestaande netwerk naar de nieuwe omgeving kan worden gemigreerd. In het design zijn geen keuzes voor de vendor gemaakt, het design is ook dermate generiek dat het te implementeren valt met apparatuur van verschillende vendors. De uiteindelijk vendor keuze zal wel bepalend zijn voor de verdere detaillering van het design.

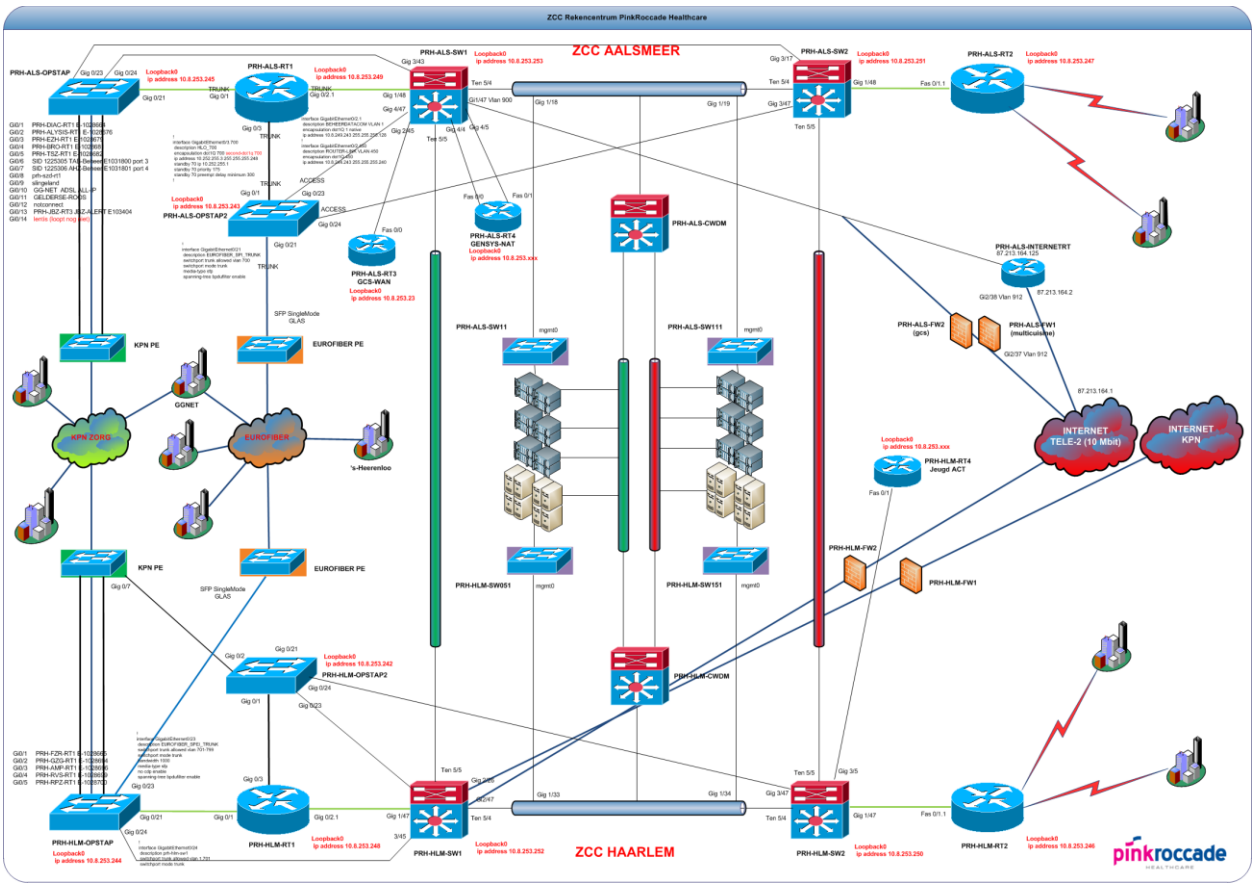
In het document is ervan uitgegaan dat de lezer een basiskennis bezit betreffende netwerkterminologie.

3. Huidige situatie

3.1. Huidig Netwerk Design

Het huidige PRHC datacenter design is een collapsed core omgeving bestaande uit vier Cisco Cat6509E L3-switches die ieder zowel een core- als distributie functie hebben. De datacenters in Haarlem en Aalsmeer hebben ieder twee Core switches. De Core switches zijn niet geclusterd en zijn door middel van een 10Gbps ethernet ring gekoppeld. Tussen de locaties wordt gebruik gemaakt een ADVA CWDM oplossing voor transport van zowel Ethernet als SAN over dezelfde glasvezelverbinding.

Aan elke Core switch is een Cisco 7206 Edge Router gekoppeld voor WAN verbindingen naar klanten via netwerken van Eurofiber en KPN-Zorg en voor verbindingen naar het internet via een Cisco ASA Firewall oplossing. De koppelingen tussen de 7206 en Cat6500 zijn 1Gbps.



Figuur 1 Huidig PRH netwerk design.

3.2. Laag 2 Switching

De huidige Core is onderdeel van een campus-brede laag 2 omgeving, elk VLAN is overal beschikbaar. Het laag 2 netwerk termineert op de Cisco 7206 edge routers en Cisco Cat6500 core switches. Er wordt gebruik gemaakt van het Cisco Rapid-PVST+ Spanning Tree protocol. Er zijn op dit moment ongeveer 600 vlans actief. De vier Core switches zijn ieder afzonderlijk spanningtree ROOT voor een eigen groep VLAN's

3.3. Laag 3 Routering

Als Laag 3 protocol wordt er gebruik gemaakt van OSPF. Er is sprake van één OSPF proces in het global routing domein en alle OSPF interfaces bevinden zich in area 6600.

Als default gateway protocol voor de core VLAN's wordt er gebruik gemaakt van HSRP waarbij alle core switches meedoen in de HSRP groepen.

3.4. Klant verbindingen naar het WAN

De WAN verbindingen naar de verschillende klantlocaties gaan via zogenaamde L2 opstap switches die gekoppeld zijn aan de 7200 Routers. De opstap switches zijn weer gekoppeld aan MPLS Provider-Edge (PE) switches van KPN-Zorg , KPN Epacity en Eurofiber.

3.5. Verbindingen naar het internet

Er zijn zowel internet koppelingen naar Tele2 als naar Signet. Tele2 verbindingen naar het internet lopen via een Cisco ASA 5520 cluster dat draait in Routed single-context mode. Dit cluster is verdeeld over de locaties Aalsmeer en Haarlem.

Verder hebben zowel Haarlem als Aalsmeer een standalone Cisco ASA 5510 die routed in single-context mode draait. Deze internet koppelingen hebben ook andere doelen of worden door andere PRH klanten gebruikt.
De ASA 5510 in Haarlem heeft een koppeling naar Signet, de ASA 5510 in Aalsmeer een koppeling naar Tele2.
De koppelingen naar de ASA's hebben een bandbreedte van 1Gbps.

In de toekomst zal de internetontsluiting via Tele-2 worden afgebouwd.

3.6. Ontsluiting Blade enclosures

Hosting van de diverse klant systemen en applicaties gebeurt met behulp van HP Blade enclosures. Ontsluiting van deze systemen gebeurd door middel van 10Gbs verbindingen naar de core switches. Intern wordt er gebruik gemaakt van HP Virtual Connect Flex10 modules om blade systemen aan de correcte VLAN's en switch poorten te koppelen.

3.7. Scheiding van klant systemen

Door de gevoeligheid van de informatie welke wordt afgehandeld binnen het datacenter is informatiebeveiliging een extreem belangrijk punt. In het huidige design wordt isolatie van de diverse klant systemen behaald door middel van VLAN's en access lists op de diverse Layer3 interfaces van de core switches. Het onderhoud van deze access lists is echter zeer arbeidsintensief.

Een ander toekomstig issue is dat door de grote hoeveelheid verschillende klantsystemen en interfaces per systeem de hoeveelheid beschikbare VLAN's op de switches sterk afneemt. Op dit moment zijn de eerste 2300 VLAN's uitgedeeld en met de verwachte groei van de komende 12 maanden zal dit snel richting de 3500 gaan.

Daarnaast maken we voor een klein aantal klanten gebruik van de VRF techniek (Virtual Routing and Forwarding) om volledige scheiding op layer 3 niveau te realiseren. Van uit beveiligingsoogpunt levert dit voor ons op het moment de beste scheiding op alleen de vraag is in hoe verre deze techniek schaalbaar is om dit toe te passen op alle klantnetwerken.

3.8. Klantverbindingen WAN

Ontsluiting naar klanten voor productie systemen vind op dit moment plaats door middel van vaste lijnverbindingen. Afhankelijk van de toepassing en wens van de klant worden er voor grote installaties een of meerdere glasvezel verbindingen neer gelegd van diverse aanbieders. Om redundantie te realiseren over deze verbindingen worden de routers binnen het datacenter en bij de klant op locatie ingericht met het HSRP protocol.
Hiermee wordt uitval van de lijnen opgevangen en wordt er automatisch overgeschakeld naar de andere verbinding.

Op dit moment wordt verkeer van verschillende klanten op verschillende vlans afgeleverd door de providers.

4. Requirements and constraints

Binnen het redesign van het netwerk komen de volgende kerndoelstellingen naar voren:

- Betere schaalbaarheid van het netwerk.
- Verbeterde robuustheid.
- Verbeterde netwerkbeveiliging.
- Vereenvoudigd beheer.

4.1. Schaalbaarheid

Naast de recente groei is de verwachting dat ook in de komende jaren de omgeving sterk zal groeien. Om dit mogelijk te maken is schaalbaarheid een bepalende factor. Op gebied van schaalbaarheid moet het ontwerp voldoen aan de volgende eisen:

- Uitbreidingen moeten eenvoudig te realiseren zijn. Dit pleit voor een modulaire opzet waarbij capaciteit kan worden uitgebreid door nieuwe apparatuur of verbindingen parallel bij te schakelen.
- Het nieuwe ontwerp moet rekening houden met technische limieten zoals die worden gesteld door bijvoorbeeld het maximale aantal vlans van 4096.

4.2. Robuustheid

Met het toenemend aantal gebruikers groeit ook het belang van een stabiele dienstverlening. Op gebied van robuustheid geldt het volgende:

- Het netwerk dient geheel dubbel te zijn uitgevoerd en door kunnen functioneren bij uitval van een onderdeel.
- Fouten in de omgeving van een klant mogen niet leiden tot problemen in de netwerkomgeving van andere klanten.

Voor optimaal gebruik van de beschikbare bandbreedte heeft een active-active opzet van redundante paden de voorkeur.

4.3. Netwerkbeveiliging

Met de groei van het aantal gebruikers wordt het ook steeds belangrijker dat de gebruikers tegen de buitenwereld, maar ook tegen elkaar beschermd zijn. Op gebied van netwerkbeveiliging moet het ontwerp voldoen aan de volgende eisen:

- Er dient een strikte scheiding te zijn tussen de diverse klantnetwerken.
- Netwerksegmenten binnen een klantnetwerk dienen eveneens door een firewall gescheiden kunnen worden,
- Verkeer afkomstig van een externe bron (klantnetwerken of internet) dient gefilterd te worden door een IPS oplossing.
- Netwerkmanagement verkeer dient gefilterd te worden door een IPS oplossing
- Dataverkeer tussen klantsystemen over het iSCSI of backup netwerk dient niet mogelijk te zijn.
- Access-lists dienen te worden vermeden. Het onderhoud hiervan is te arbeidsintensief.

4.4. Beheer

Voor netwerkbeheer is het van belang dat dit zo eenvoudig mogelijk is om de beheerinspanning beperkt te houden. De manier om dit te bereiken is sterke standaardisatie van de oplossing zowel in techniek als in de procedures. Dit document behandeld de technische kant van deze standaardisatie maar dient wel aangevuld te worden door PRH zelf met ondersteunende standaardprocedures.

4.5. WAN verbindingen

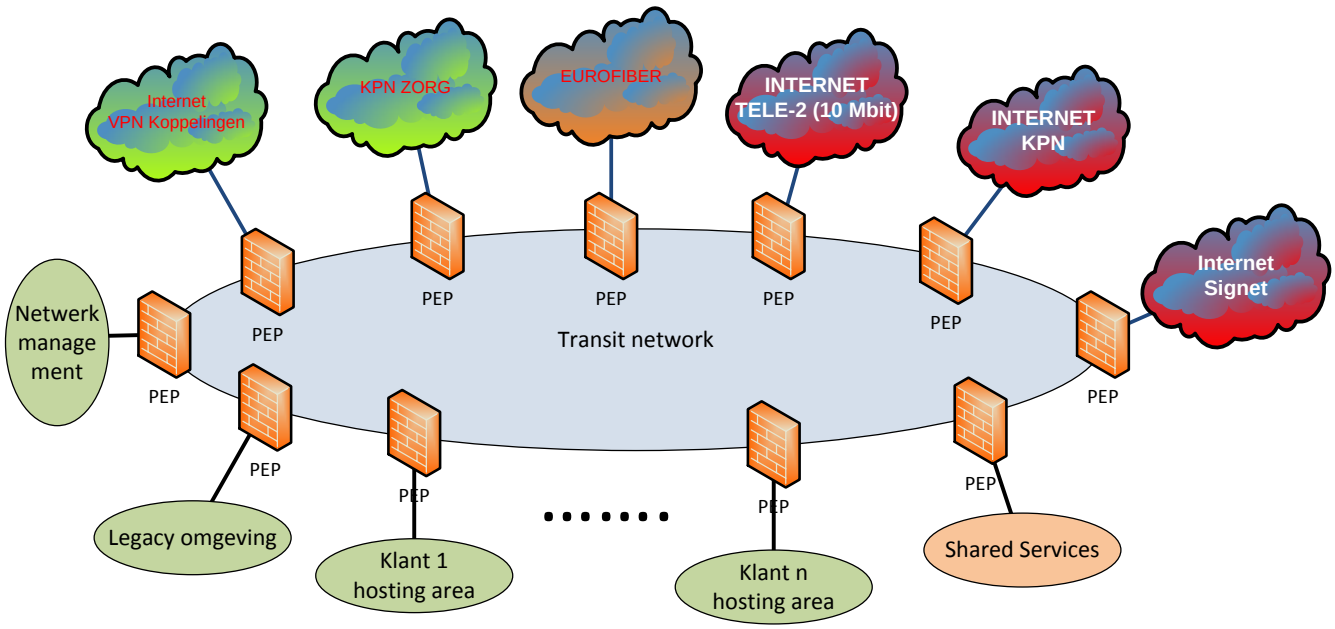
WAN verbindingen zijn nu redundant door gebruik van het HSRP protocol. In de huidige situatie resulteert dit in een active-standby opzet waarbij slechts een van de lijnen actief wordt gebruikt. Een wens hier is de mogelijkheid om de lijnen active-active te gebruiken en hiermee de beschikbare lijncapaciteit voor redundant gekoppelde klanten te verdubbelen.

4.6. Fysieke beperkingen

De nieuwe infrastructuur zal lange tijd naast de bestaande infrastructuur functioneren. Uitbreidingen in de vorm van extra kasten en nieuwe bekabeling is kostbaar en dient indien mogelijk vermeden te worden.

5. Design

Om een schaalbaar design te krijgen is gekozen voor een ontwerp op basis van het Adaptive Network Architecture. Hierbij worden alle zones dmv een Policy Enforment Point gekoppeld aan een transit network.

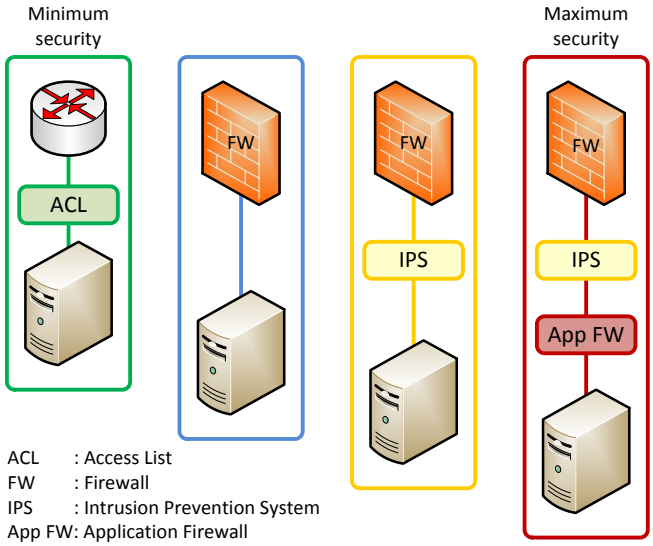


Figuur 2 High level view van de nieuwe netwerkstructuur.

Bovenstaand figuur geeft deze opzet weer. Niet alle externe segmenten zijn hier overigens op vermeld. Elk klant hosting area bevat een aantal zones opnieuw gekoppeld met een transit network. Deze zones zijn bijvoorbeeld de klant DMZ, klant productie, klant test en klant acceptatie. De verschillende zones zijn opnieuw met een PEP gekoppeld.

5.1.1. PEP's

De Policy Enforcement Points zijn de basis van de netwerkbeveiliging. Een PEP kan op verschillende manieren worden uitgewerkt, van een eenvoudige access-list tot een combinatie van IPS, Firewall en applicatie firewall.

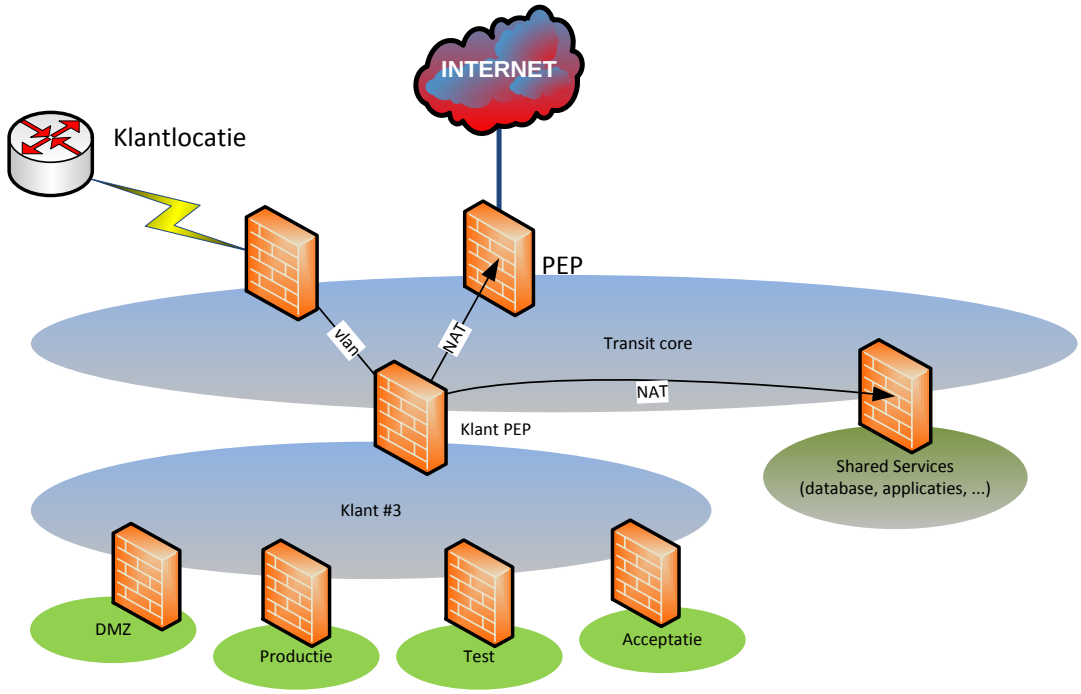


Figuur 3 Policy Enforment Point opties

Bovenstaand figuur geeft de verschillende mogelijkheden. In dit ontwerp wordt geen gebruik gemaakt van access lists vanwege het moeizame beheer van deze vorm van beveiliging. Voor koppelingen naar buiten, richting klant of internet wordt een combinatie van firewall en IPS gebruikt. Voor interne scheiding wordt alleen een firewall instance gebruikt. Voor netwerk management verkeer wordt eveneens een IPS firewall combinatie gebruikt.

5.1.2. Klant hosting area

De klant specifieke apparatuur wordt geplaatst in de klant hosting area. Afhankelijk van de compexiteit van de omgeving kan een hosting area weer uit meerdere zones bestaan.

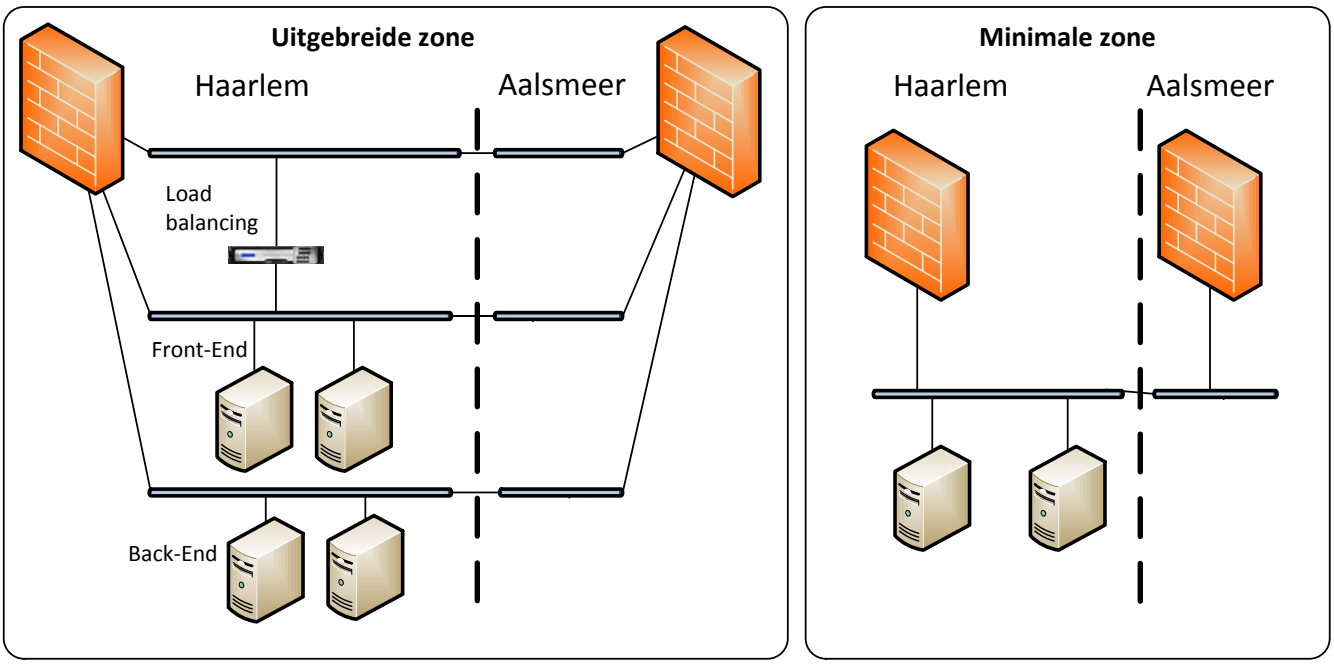


Figuur 4 Opzet klantsegment.

De koppeling van de klant naar externe locaties en diensten loopt via het klant PEP. Door op de verbinding naar internet en common services Network Address Translation (NAT) toe te passen worden problemen met eventueel overlappende IP ranges tussen klanten voorkomen.

Binnen een klant hosting area kunnen weer meerdere zones voorkomen. Een produktiezone kan bijvoorbeeld weer uit meerdere segmenten bestaan waarbij de verschillende segmenten door een firewall gescheiden zijn. De vlans zijn gestretched over beide data center locaties. Klantsystemen kunnen zo over beide locaties verspreid zijn.

In onderstaand figuur vindt standaard alle communicatie plaats in het Haarlem data center. Bij het falen van de Haarlem firewall wordt de Aalsmeer firewall gebruikt.



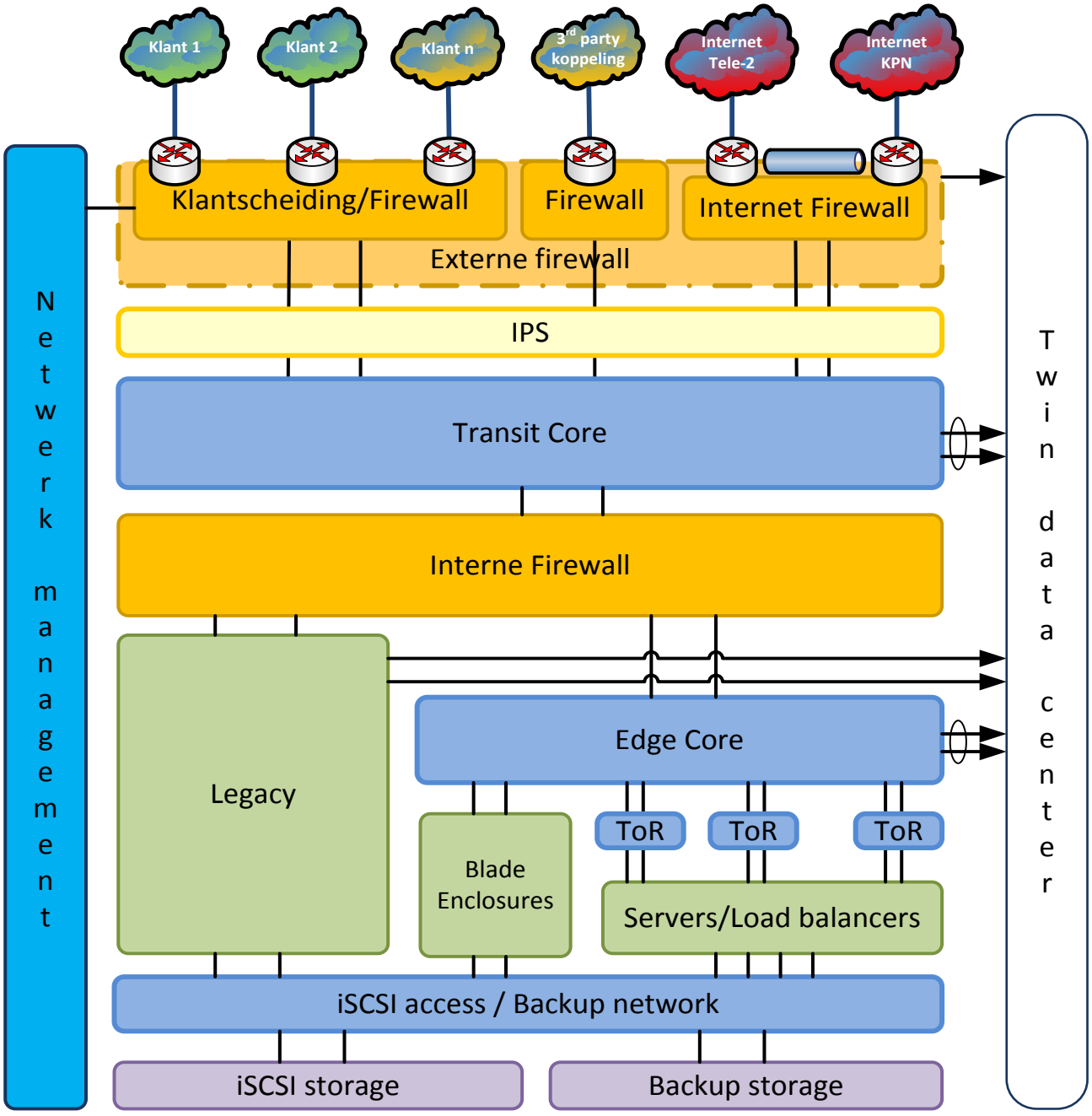
Figuur 5 Voorbeelden van de invulling van een zone.

In het load-balancer segment is de back-end van de load-balancer gekoppeld op het Front End serversegment. De reden hiervan is dat er meestal geen security issues tussen beide segmenten spelen en dat hierdoor wel extra communicatie door de firewall wordt vermeden.

In het nieuwe klant hosting plaatje zal de Citrix Netscaler geen SSL offloading meer doen. Dit gebeurt nu op de rand van het data center netwerk. De andere Netscaler functies blijven gehandhaaft.

5.2. Verdere uitwerking van het design.

Het logische plaatje in Figuur 2 wordt uitgewerkt tot het blokdiagram in Figuur 6. Hier wordt voor een locatie aangegeven hoe de verschillende onderdelen koppelen. De Transit core bevat de koppelingen naar alle deelnetwerken. De deelnetwerken zelf, klantnetwerken en common applications bevinden zich achter de interne firewalls op de Edge core omgeving. In de volgende paragrafen wordt het design blok voor blok verder uitgewerkt.



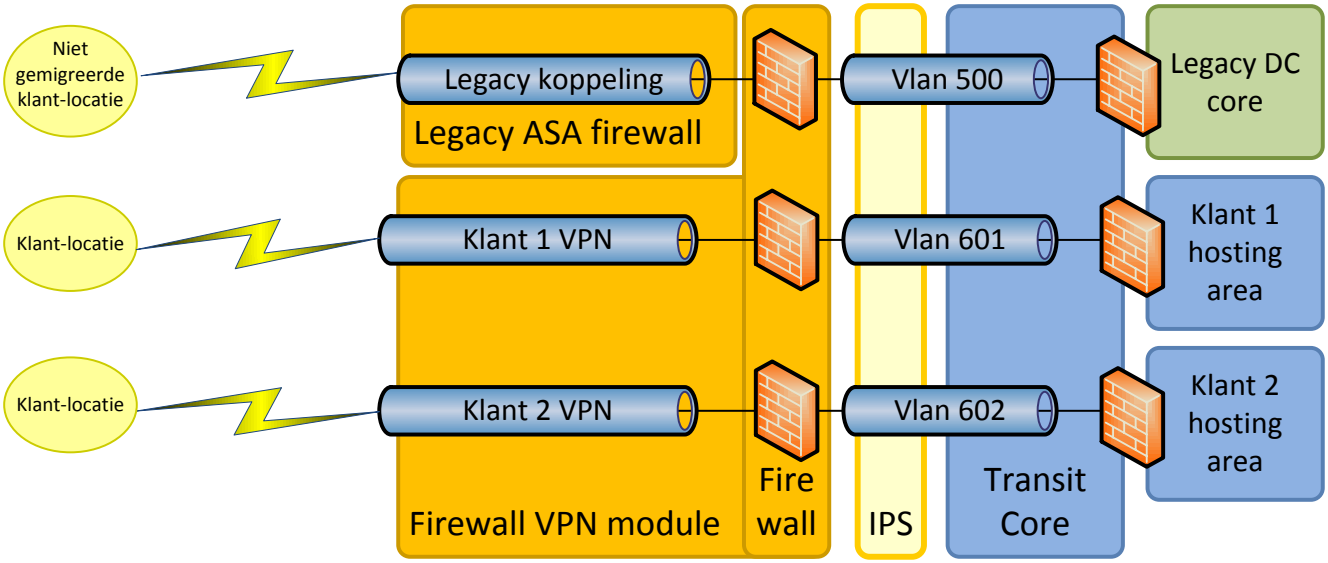
Figuur 6 Basis data center design.

5.3. Externe firewall

De externe firewall koppelt Wan- en Internetverbindingen op de Transit core. Een drietal verschillende verbindingen wordt op de firewall afgeleverd, klantverbindingen, 3rd party verbindingen en de verbindingen naar internet.

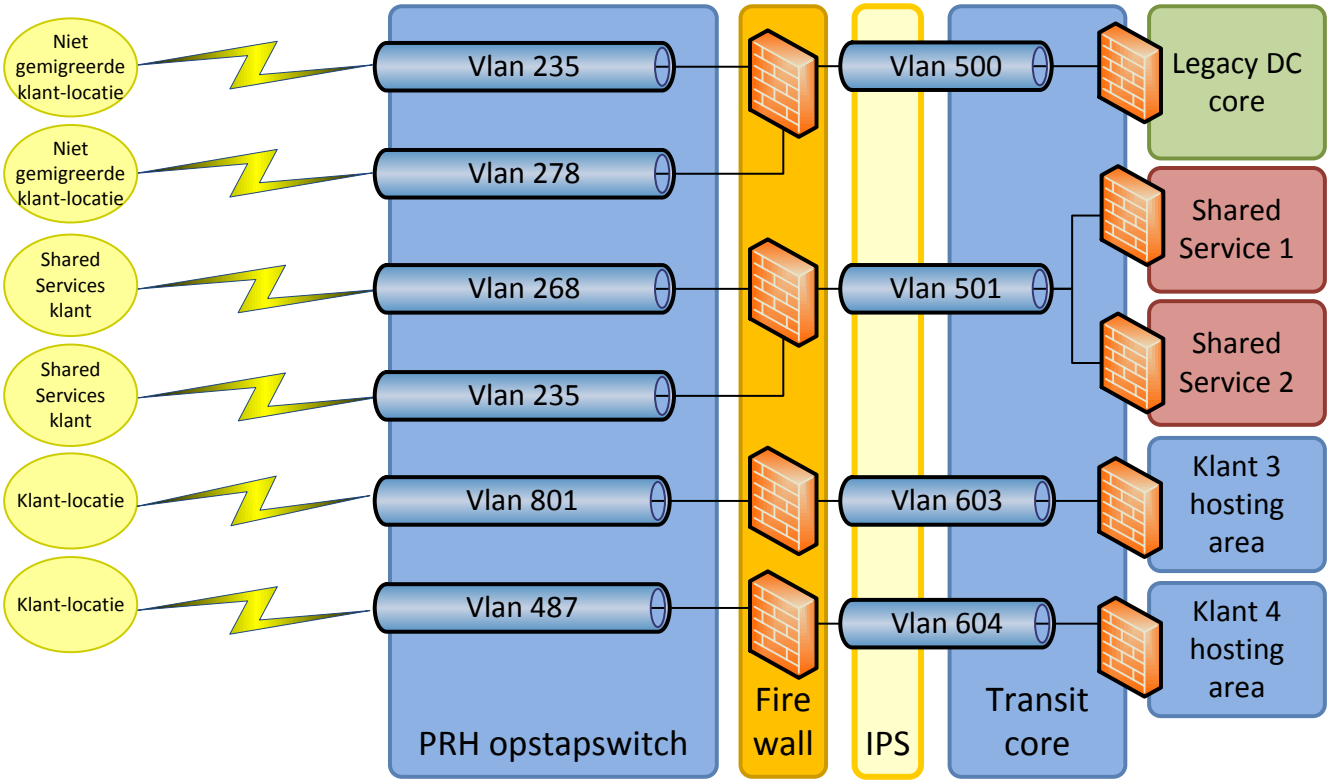
5.3.1. Klantscheiding/Firewall

Op dit punt wordt het verkeer van de verschillende klanten gescheiden zodra het binnenkomt via KPN zorg, Eurofiber of de internet vpn's. Verkeer voor elke klant komt binnen via de opstap switches op een apart vlan. Dit vlan wordt doorgezet door de IPS en Transit core en wordt uiteindelijk aangeboden op de klant firewall. Wanneer het verkeer niet expliciet wordt benoemd wordt het aangeboden op de firewall van de legacy omgeving. Direct na de eerste implementatie van het ontwerp zal dat nog gelden voor vrijwel al het dataverkeer.



Figuur 7 Klantscheiding op de PRH Edge voor internet VPN's.

Al het klantverkeer wordt gescand door de IPS, de firewall bevat een aantal globale rules bedoeld om een eerste filtering van het netwerkverkeer te maken. Het idee is dat deze firewall alleen hoeft te worden aangepast voor nieuwe klanten of nieuwe diensten. Detailfiltering van het verkeer vind pas later plaats op de klant firewall.

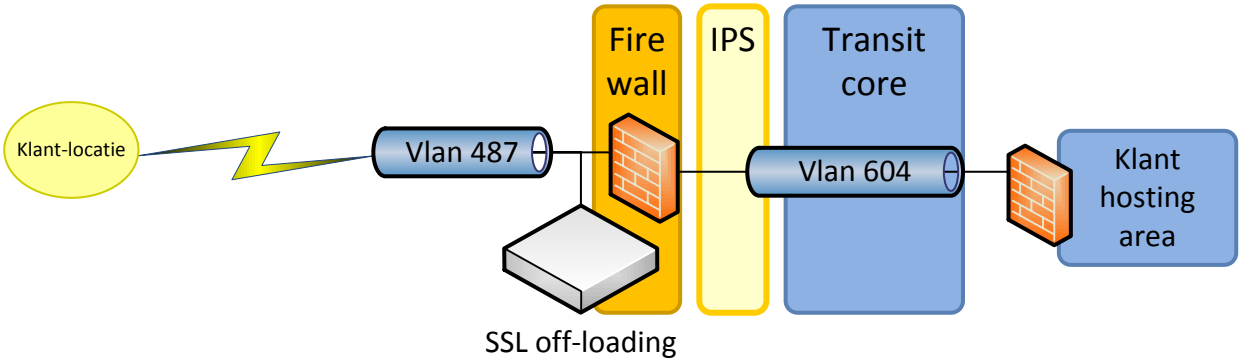


Figuur 8 Klantscheiding op de PRH edge via de opstap switches.

Om een gestructureerde vlan omgeving op de transit core te kunnen bieden worden de firewalls in layer-3 mode geplaatst. Op die manier kan de anders gestructureerde vlanindeling aangeboden door de providers omgezet worden naar een eenduidige vlanindeling op de transit core. Bovendien kunnen doublures in vlangebruik bij verschillende providers (bijvoorbeeld vlan 235 in Figuur 8) worden opgevangen.

Een aantal klanten heeft geen eigen hosting area maar koppelt op een common application omgeving. De vlans voor deze klanten worden afgeleverd op de common application omgeving.

Op dit moment worden de internet VPN's geconfigureerd op de externe Cisco 7200 switches. In de nieuwe opzet kan deze functie op de firewall worden gezet zoals aangegeven in Figuur 7.

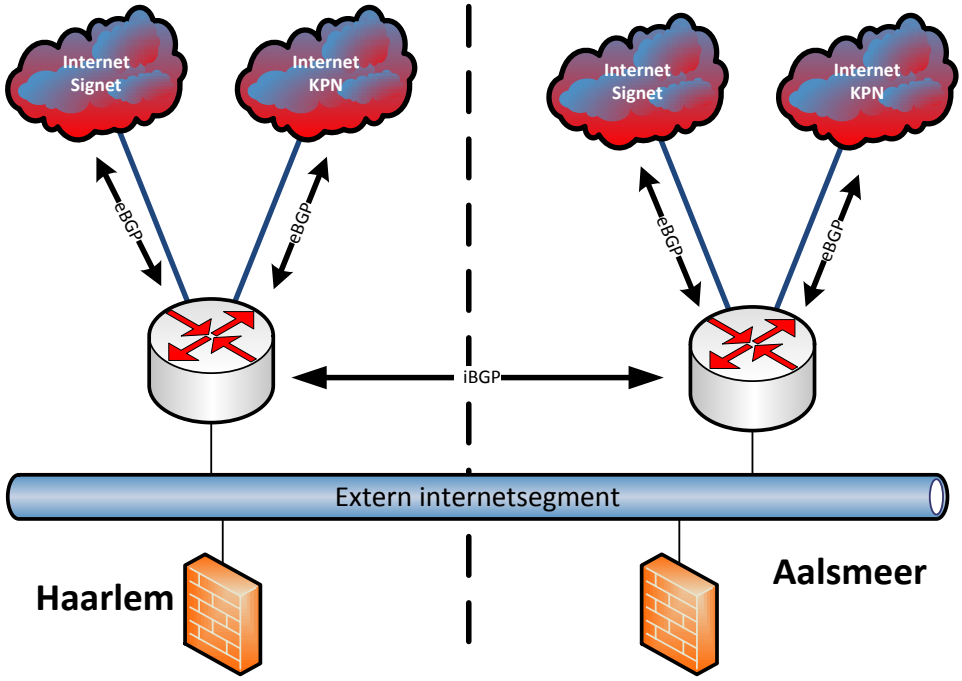


Figuur 9 SSL offloading voor de firewall.

In de huidige situatie vind SSL offloading plaats op de Citrix Netscalers die in de klant hosting area geplaatst gaan worden. Dit heeft tot gevolg dat er encrypted SSL-tunnels van de klant-locatie tot in de klant hosting area lopen die niet geinspecteerd kunnen worden door IPS en firewalls Om dit te voorkomen dient SSL offloading voor (of op?) de externe firewall plaats te vinden zodat de firewall en IPS het inkomende verkeer kunnen scannen.

5.3.2. Internet firewall/3rd party firewall

De internet firewall functioneert als een traditionele internet firewall. Binnenkomend verkeer wordt standaard geblokkeerd met uitzondering van benoemde (DMZ) diensten. De koppelrouters naar internet kunnen in de toekomst worden geconfigureerd met BGP om meer controle te krijgen of internetverkeersstromen en een betere redundantie te bieden.



Figuur 10 Externe routering met BGP.

Om een BGP koppeling te maken moet een Autonomous System (AS) nummer worden aangevraagd en moeten met Signet en KPN afspraken worden gemaakt over de koppeling. Providers bieden in het algemeen ondersteuning bij het configureren van BGP maar binnen de eigen organisatie moet zeker kennis aanwezig zijn over BGP.

De 3rd party firewall koppelt diensten zoals Gemnet aan het data center.

De Internet en 3rd party firewalls kunnen zowel als layer-2 als layer-3 firewalls worden geplaatst. De complexiteit van de migratie zal waarschijnlijk bepalend zijn voor de keuze.

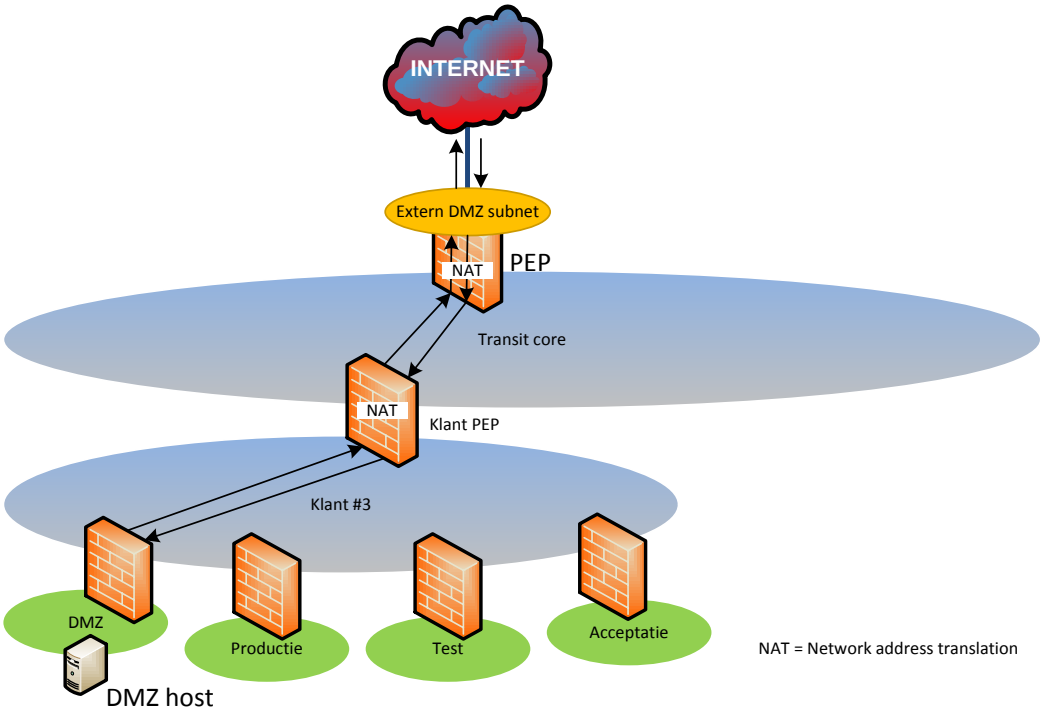
5.3.3. Routering

De routering van de klant kan met OSPF worden doorgetrokken naar de klant hosting area. Klanten met een PRH edge router op de klantlocatie kunnen load-balancing naar de data centers op basis van OSPF loadbalancing configureren. Statische routering is hiervoor niet geschikt.

Afhankelijk van het gekozen model firewall is asymmetrische routering door de firewalls een probleem. Wanneer aan de klant kant de routering correct is dan wordt verkeer over dezelfde verbinding teruggestuurd als waarover dit verkeer binnenkwam. Wanneer gekozen wordt voor een volledig redundante firewall waarbij de firewall cluster één ip adres en één MAC adres gebruikt is assymetrisch routering geen issue.

5.3.4. DMZ gebruik

PRH host ook publieke webservers voor klanten. Deze webservers maken gebruik van publieke adressen uit een PRH IPv4 subnet. In het nieuwe plaatje staan de DMZ servers in de klant hosting area's. Dit betekent dat de publieke adressen vertaald moeten worden naar interne private adressen waarna het verkeer naar de betreffende webserver gestuurd dient te worden. Op de tussenliggende firewalls vindt netwerk adres vertaling (NAT) plaats.



Figuur 11 Toegang tot DMZ systemen vanaf internet.

Om redundancy voor het interne DMZ segment te realiseren wordt VRPP of de cluster faciliteit van het gekozen model firewall gebruikt.

5.3.5. Hardware invulling

Voor de firewall functies in klantscheiding, 3rd party firewall en de internet firewall kan een fysieke firewall cluster worden gebruikt met verschillende contexten, een per functie. Elke data center locatie heeft dan een element van de cluster.

De totale capaciteit van de firewall moet minimaal gelijk zijn aan de som van de connection speeds van de gekoppelde Wan en internetverbindingen. Gezien de aard van deze verbindingen is latency een minder belangrijke factor voor deze firewall. Wanneer internet VPN's worden gemigreerd van de routers naar de firewalls dan moeten de firewalls deze VPN's ook in de gewenste aantallen ondersteunen.

De verbinding van het externe internetsegment naar de twin data center locatie loopt via een vlan op de nieuwe core switches.

Schaalbaarheid: Om meer verbindingen of meer bandbreedte te kunnen faciliteren kunnen nieuwe fysieke firewalls parallel worden bijgeplaatst en kunnen firewall contexten eventueel worden verhuisd.

Robuustheid: Op beide data center locaties worden de externe koppelingen gemaakt. Bij uitval van een koppeling wordt automatisch de koppeling op de twin data center locatie gebruikt. BGP kan een verbeterde internet redundantie en efficienter gebruik van de internetcapaciteit bieden.

Beheerbaarheid: De firewall context configuraties zijn in hoge mate statisch. Voor nieuwe klanten zal de klantkoppeling moeten worden geconfigureerd.

Beveiliging: De firewall vormt samen met de IPS de eerste beveiligingslaag voor extern verkeer.

5.4. IPS

De IPS (Intrusion Protection System) filtert het verkeer dat van buiten het datacenter afkomstig is en het verkeer tussen het netwerk-management netwerk en de transit core. De IPS wordt op laag 2 tussengekoppeld. De capaciteit van de IPS moet minimaal gelijk zijn aan de som van de connection speeds van de verschillende gekoppelde WAN- en internetverbindingen.

Schaalbaarheid: Om meer verbindingen of meer bandbreedte te kunnen faciliteren kunnen nieuwe fysieke IPSsen parallel worden bijgeplaatst.

Robuustheid: Op beide data center locaties wordt een IPS geplaatst. Bij uitval van een IPS vallen de externe verbindingen op een locatie weg en worden de verbindingen op de twin data center locatie gebruikt. Een voorziening om uitval van een IPS lokaal op te vangen is echter aan te raden.

Beheerbaarheid: De IPS configuratie is in hoge mate statisch, nieuwe signature files kunnen automatisch worden gedownload en geimplementeerd.

Beveiliging: De IPS vormt samen met de firewall de eerste beveiligingslaag voor extern verkeer.

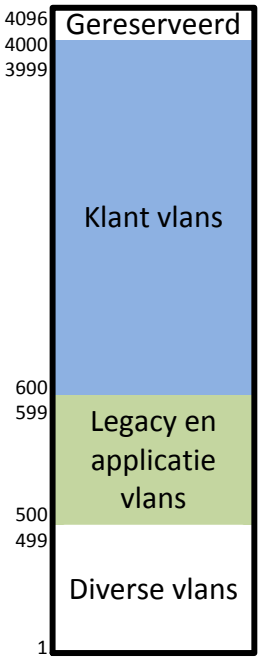
5.5. Transit core

De transit core is de virtual backbone in het Adaptive Networking Architecture concept. Verkeer dat al gescheiden is wordt over de transit core zonder routering doorgezet naar de klant firewalls. Verkeer voor de Legacy omgeving, voor applicatie en database services en voor internet wordt binnen de transit core op de core router naar de firewalls gerouteerd. Het gehanteerde routeringsprotocol is OSPF. De transit core vormt area 0 voor OSPF, via de firewall koppelt dit naar de legacy OSPF area 6600.

De core router dient ter ontlasting van de firewalls. Op alle firewalls kan nu een default gateway naar de transit core router worden gezet. Alleen firewalls waarachter routerbare vlans aanwezig zijn dienen met OSPF te communiceren. Dit geldt voor de Common Application firewalls, de internet en 3rd party firewalls. Beide locaties, Aalsmeer en Haarlem hebben hun eigen core router.

Voor koppelingen naar firewalls en andere componenten wordt indien mogelijk het Link Aggregation Control Protocol gebruikt (LACP). Dit protocol combineert meerdere fysieke verbindingen tot één logische verbinding. Bij uitval van een fysieke verbinding wordt het verkeer over de overblijvende verbindingen gestuurd.

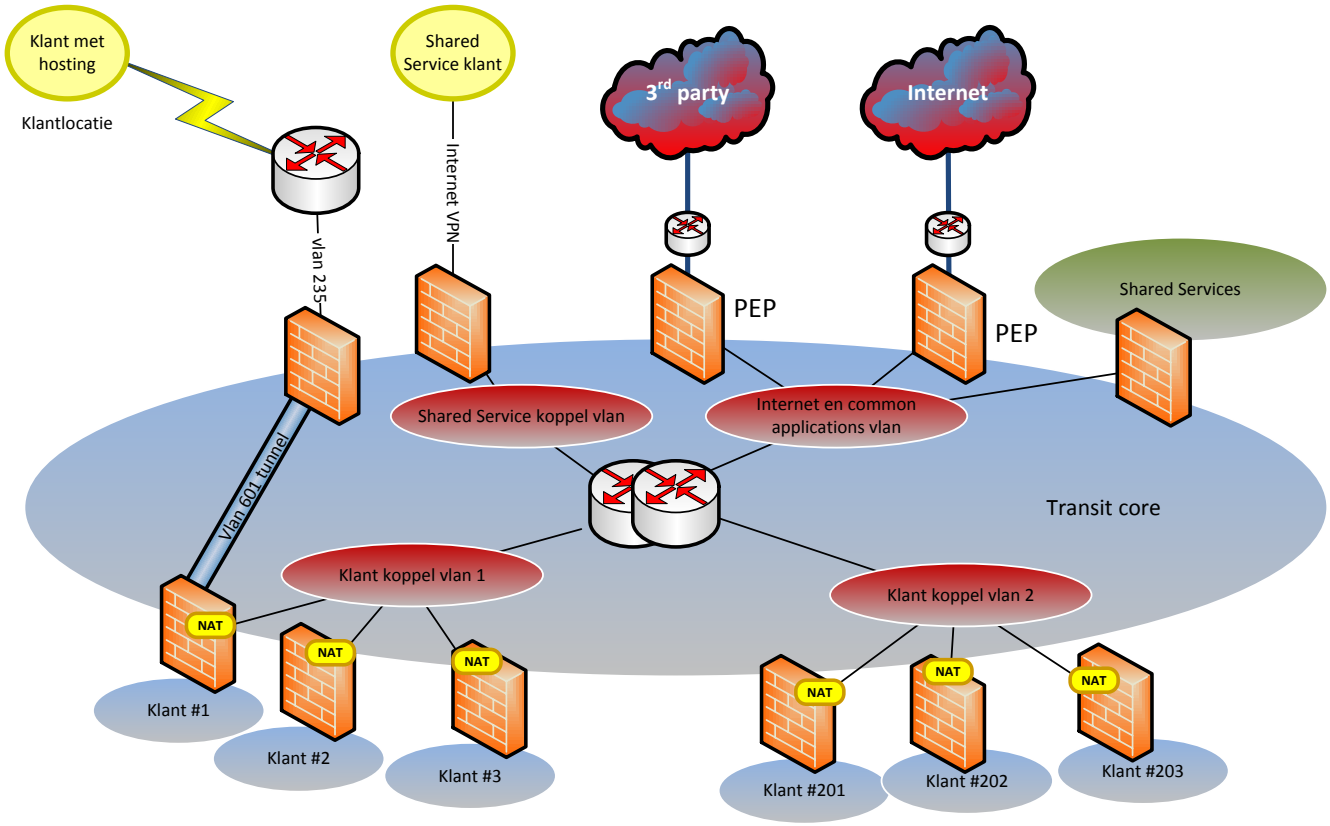
Alle vlans worden gestretched over beide DC locaties.



Figuur 12 Transit core vlanindeling.

Vlans

De transit core en de interne en externe firewalls vormen één vlan domein. De interne firewall vormt de grens met het vlan domein van de Legacy omgeving. Op deze manier wordt de nieuwe vlan structuur gescheiden van de bestaande vlan structuur op de legacy omgeving. Een mogelijke indeling voor de transit core vlans is gegeven in Figuur 12



Figuur 13 Transit core opzet

Hardware invulling

De transit core bestaat uit een stack van twee of meer 10 gigabit switches. Dit kan een aparte set core switches zijn maar kan ook een context zijn op een set switches die de transit core en de edge core huisvest. Op deze manier wordt optimaal met ruimte en poortcapaciteit omgegaan.

De transit core is met een dubbele 10 Gbit link via de ADVA CWDM oplossing gekoppeld aan de transit core op de twin data center locatie.

Schaalbaarheid: Om meer verbindingen of meer bandbreedte te kunnen faciliteren kunnen nieuwe switches in de stack worden bijgeplaatst.

Robuustheid: Bij uitval van een switch blijft de rest van de switch stack functioneren. De koppelingen naar de firewalls en de twin data center locatie is een LACP trunk over meerdere switches zodat bij uitval van een switch de verbinding blijft bestaan. Alleen de beschikbare bandbreedte wordt minder. De routeringsfunctie bevindt zich op de redundante switch stack en zal dus eveneens redundant zijn.

Beheerbaarheid: Door het gebruiken van standaard configuraties voor het koppelen van nieuwe klanten en diensten wordt het beheer sterk vereenvoudigd.

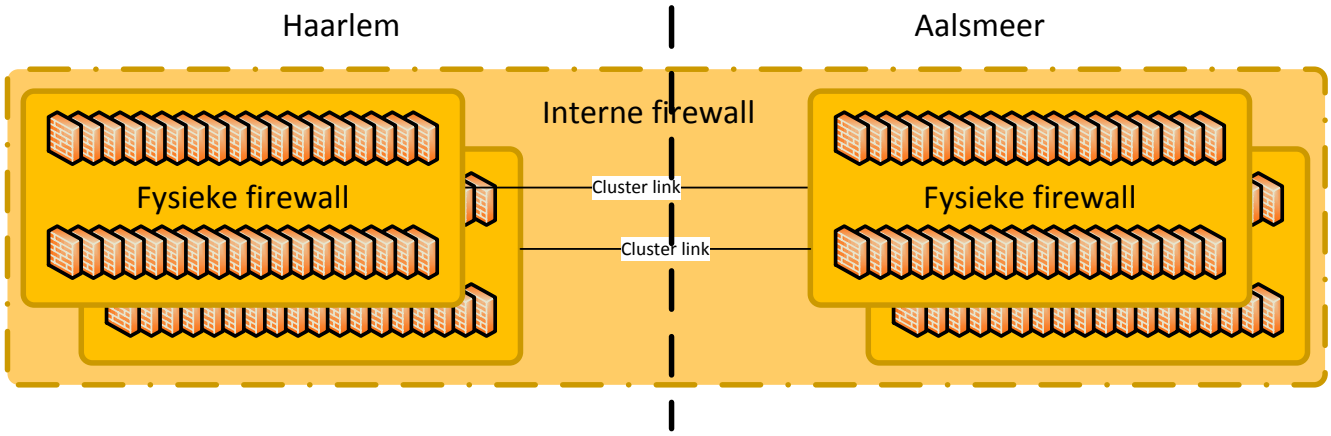
Beveiliging: De Transit core kent zelf geen beveiliging. Management toegang is alleen mogelijk vanaf het netwerk management segment.

5.6. Firewall segment

Het firewall segment is het meest kritische deel van dit design. Voor elke gehoste klant zijn in dit segment één of meerdere virtuele firewalls gedefinieerd. Verkeer binnen de hosting area tussen verschillende zones wordt eveneens door de firewall gerouteerd. Dit ontwerp heeft een aantal aandachtspunten:
Verkeer binnen de hosting area en naar andere delen van het data center passeert meerdere firewalls. De opgetelde latency (netwerkvertraging) veroorzaakt door elke firewall kan hierdoor voor een flinke vertraging van het dataverkeer zorgen. Het is dus van belang dat deze firewalls een minimale latency hebben en dat rulebases klein zijn en geoptimaliseerd zijn voor snelheid.

Het grote aantal firewalls en segmenten kan betekenen dat er al snel limieten worden geraakt zoals maximale aantal contexten binnen een bepaalde fysieke firewall. De oplossing is dan om een nieuwe set fysieke firewalls te plaatsen. Bij de keuze van de firewall is dus ook van belang dat de firewall voldoende contexten aankan.

Tenslotte is de throughput van de firewall van groot belang. Intern data verkeer wordt vaak meerdere keren geprocessed door de firewall.



Figuur 14 Geclusterde firewall opzet.

De firewall wordt geclusterd met een tweede firewall op de twin data center locatie. De clustering is bij voorkeur op basis van IP/MAC takeover om configuratie van het netwerk rondom de cluster eenvoudig te houden. Wanneer dit niet beschikbaar is dan wordt deze functionaliteit met VRRP geimplementeerd (Wat dan wel beschikbaar moet zijn op de firewall.)

In een data center opzet moet vaak een keuze worden gemaakt tussen losse firewall appliances of blades in een high speed core. De laatste oplossing wordt door dit ontwerp vrijwel uitgesloten. Voor redundantie zijn de core switches dubbel uitgevoerd per locatie. De firewall is echter redundant over verschillende locaties. Wanneer blades worden gebruikt zijn er dus één blade en twee core switches per locatie. Plaatsing van de blade in een van de cores is mogelijk maar compliceert de redundancy.

De internet- en klant firewall functionaliteit wordt bij voorkeur op een fysiek andere firewall dan de interne firewall geplaatst. Dit maakt het ook mogelijk om een dual vendor firewall policy te hanteren waarbij externe firewalls van vendor 1 en interne firewalls van vendor 2 zijn. Een vulnerability op een firewall model geeft op deze manier geen toegang tot het hele netwerk maar stopt deze op de Transit core. Het is desalniettemin wel mogelijk om alle firewall functionaliteit op dezelfde fysieke firewall te implementeren.

Schaalbaarheid: Om meer verbindingen of meer bandbreedte te kunnen faciliteren kunnen nieuwe fysieke firewall clusters parallel worden bijgeplaatst.

Robuustheid: Bij uitval van een firewall neemt de clusterpartner het over. Er zal dan wel een groot deel van het verkeer over de link tussen de locaties lopen wat een performancevermindering van applicaties kan opleveren.

Beheerbaarheid: Het merendeel van de klantconfiguratie zal op deze firewalls plaatsvinden. Door het gebruiken van standaard configuraties voor het koppelen van nieuwe klanten en diensten wordt het beheer sterk vereenvoudigd.

Beveiliging: De interne firewall scheidt de verschillende klantnetwerken en beperkt het verkeer tussen de verschillende segmenten van een klant hosting area.

Hardware invulling

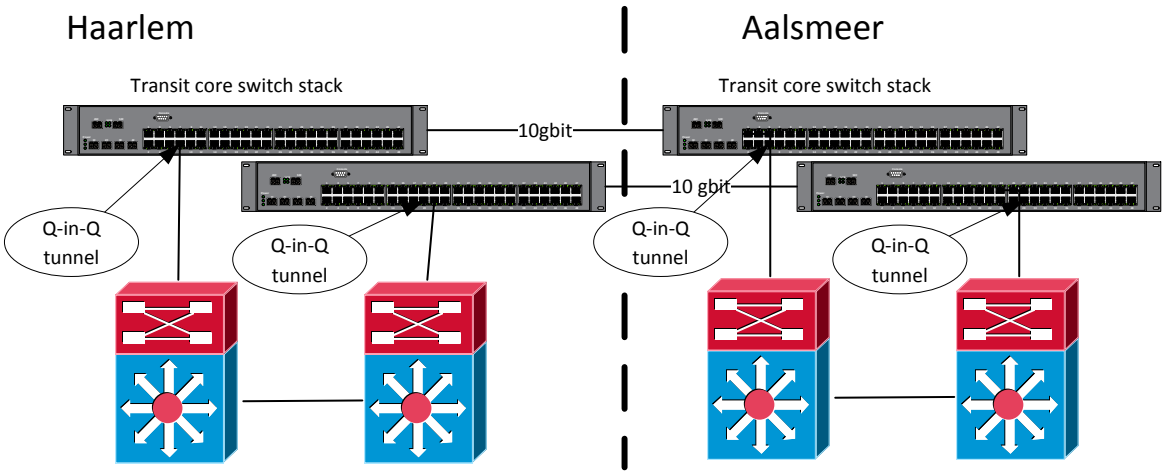
Eisen aan de interne firewall zijn:

- Lage latency zodat verkeer tussen Front End en Back End servers zo min mogelijk vertraagd wordt.
- Moet minimaal enkele honderden virtuele contexten aankunnen (hoe meer hoe beter).
- Maakt onderscheid tussen vlans op basis van binnenkomend interface.

De laatste eis heeft betrekking op de scheiding tussen vlan domeinen.De firewall is eveneens de scheiding tussen de vlan domeinen van de Transit core en de Edge core(s). Dit betekent dat wanneer een vlan 1000 wordt aangeboden op de Transit core interface dit niet gezien mag worden door de firewall als hetzelfde vlan 1000 op het Edge core interface.

5.7. Legacy segment

De bestaande Data centeromgeving zoals die ontsloten wordt door de vier 6500 core switches vormt het legacy segment. Alle externe koppelingen zijn verplaatst naar de externe firewall laag. De verbindingen naar extern verlopen nu door de Legacy firewall en de transit core. De verbindingen naar de iSCSI omgeving lopen via het iSCSI netwerk.



Figuur 15 Legacy site-to-site koppeling.

De Legacy omgeving is gekoppeld met 2x 10Gbit naar de twin data center locatie. Deze koppeling loopt met een Q-in-Q link via de transit core. Op deze manier wordt vermeden dat er extra 10 Gbit verbindingen nodig zijn die anders slechts nominaal worden belast.

Schaalbaarheid: nvt.

Robuustheid: De Legacy omgeving is dubbel gekoppeld en zal even robuust functioneren als voor de implementatie van het nieuwe design.

Beheerbaarheid: Deze zal identiek zijn aan de situatie voor de migratie.

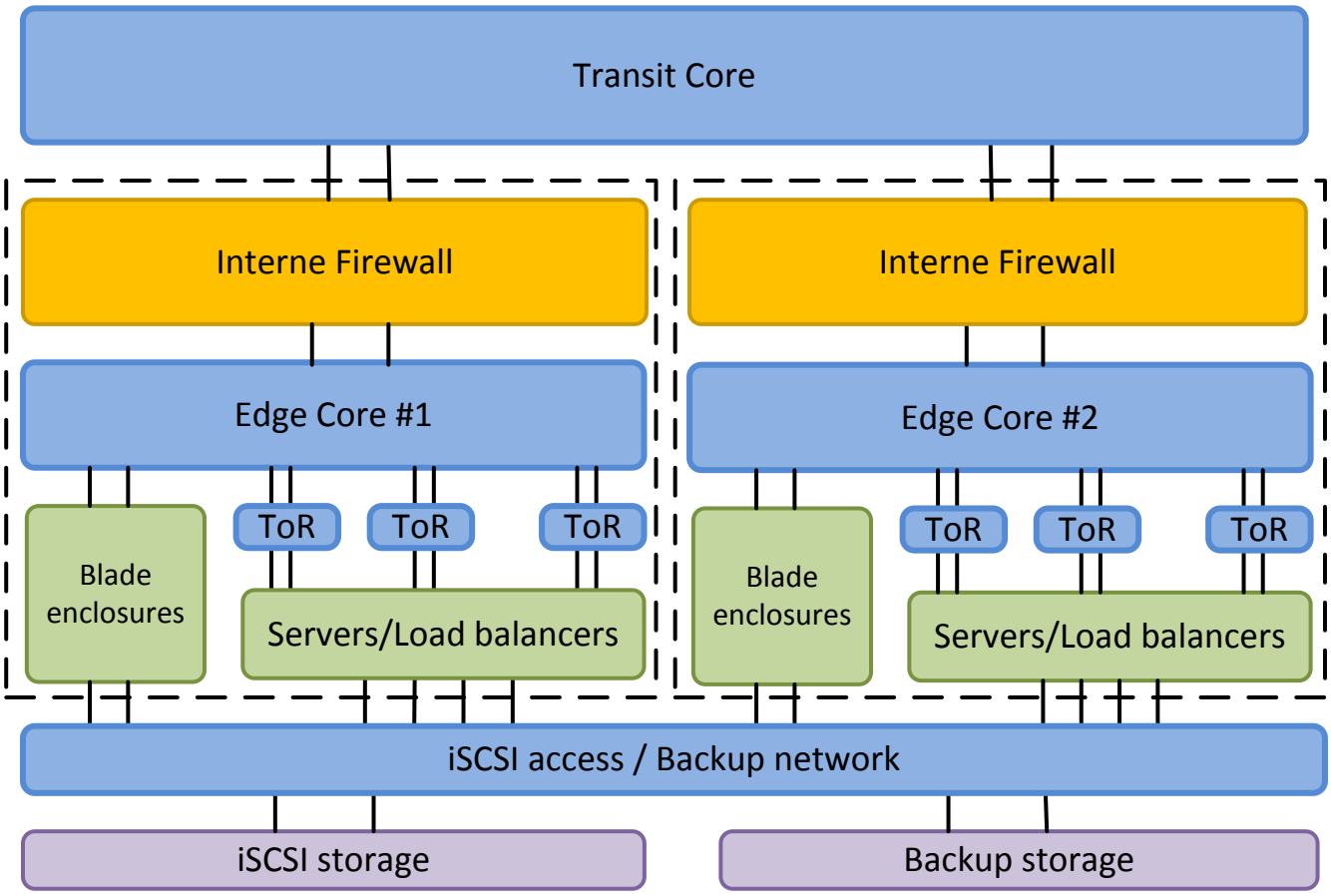
Beveiliging: De externe en interne firewall en de IPS schermen ook de Legacy omgeving af.

5.8. Edge switch core

Er is gekozen voor een Top of Rack benadering waarbij elk rack voorzien wordt van een redundante set switches gekoppeld met stack technologie tot een virtuele switch. Voordeel van deze methode is dat er minder kabels tussen de racks onderling nodig zijn en dat de uiteindelijk core switches met minder poorten toe kunnen.

De Edge switch core is een 10 Gbit switch stack waarop de verschillende Top of Rack switches met een LACP verbinding redundant worden gekoppeld. De stack is vooral een snelle laag-2 switch.

Op de Edge core omgeving wordt het grootst aantal vlans verbruikt. Wanneer er onvoldoende vlans ter beschikking zijn dan kan een nieuwe Edge core worden toegevoegd, los van de bestaande. Deze moet ook gekoppeld worden aan een aparte fysieke interne firewall cluster en uitgerust worden met eigen Top of Rack switches. Door de apparatuur in de racks per Edge Core te organiseren kan voorkomen worden dat meerdere sets Top of Rack switches in een kast nodig zijn. Figuur 16 geeft aan hoe de schaalbaarheid vorm gegeven wordt.

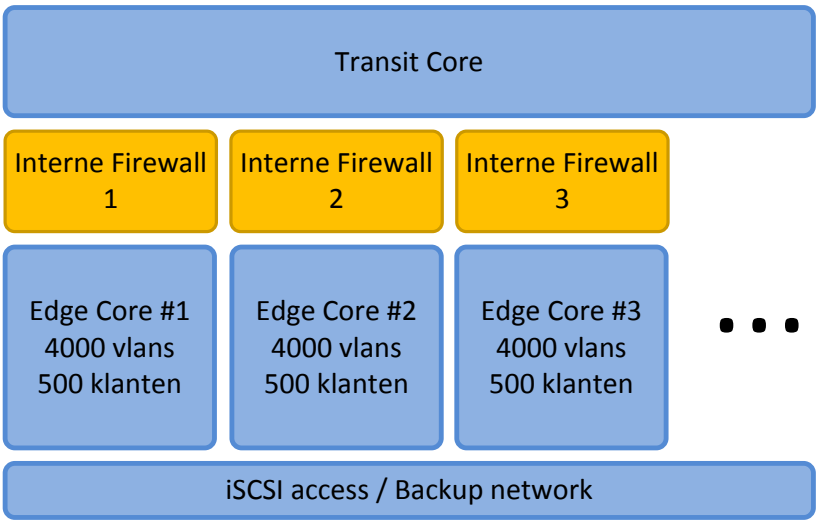


Figuur 16 Uitbreiding door toevoegen van een extra Edge core omgeving.

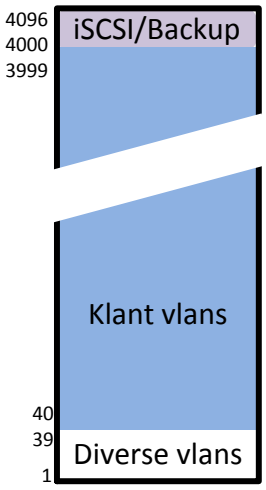
De nieuwe Edge core zelf kan eventueel worden gecreëerd door opnieuw een context op de bestaande switch core stack aan te maken.

Figuur 18 geeft een mogelijke vlanindeling voor de Edge core omgevingen.

Een nieuwe Edge core omgeving vereist ook eigen 10 Gbit verbindingen tussen de data centers. Deze kunnen echter net als de Legacy omgeving via een Q-in-Q tunnel gerealiseerd worden.



Figuur 17 Schaling Edge core omgeving.



Figuur 18 Vlan indeling per Edge core.

Hardware invulling
Uit efficiency en kastruimte overwegingen is het aan te bevelen de Transit en Edge switch core als contexten op één set fysieke switches te plaatsen.

Schaalbaarheid: Om meer verbindingen of meer bandbreedte te kunnen faciliteren kunnen nieuwe switches in de stack worden bijgeplaatst.

Robuustheid: Bij uitval van een switch blijft de rest van de switch stack functioneren. De koppelingen naar de firewalls en de twin data center locatie is een LACP trunk over meerdere switches zodat bij uitval van een switch de verbinding blijft bestaan. Alleen de beschikbare bandbreedte wordt minder.

Beheerbaarheid: Door het gebruiken van standaard configuraties voor het koppelen van nieuwe klanten en diensten wordt het beheer sterk vereenvoudigd.

Beveiliging: De Edge core kent zelf geen beveiliging. Management toegang is alleen mogelijk vanaf het netwerk management segment. Verkeer van de verschillende klanten is op vlan basis van elkaar gescheiden.

5.8.1. Edge/Top of Rack switches
De edge switches worden gebruikt als layer 2 switches en bieden UTP gigabit poorten voor serveraansluitingen en 10 Gbit SFP+ interfaces voor de koppelingen naar de data en de iSCSI-core switches. Eventuele blade enclosures en andere apparatuur die met 10 Gbit glas wordt gekoppeld wordt rechtstreeks op de core gekoppeld.

Om het aantal switches in een kast te beperken worden de edge switches gebruikt voor het datanetwerk, het iSCSI netwerk en voor het backup netwerk. De iSCSI functie is het meest veeleisend en dicteert de keuze van de switch. iSCSI vereist dat de switch grote buffers en flow control ondersteunt. Een standaard netwerk switch heeft een poortbuffer van enkele megabytes. Een iSCSI switch heeft vaak een poortbuffer van een of enkele gigabytes.

Schaalbaarheid wordt verkregen door het toevoegen van een of meer extra switches in de stack. Hiermee komen dan ook meer 10 Gbit SFP+ poorten beschikbaar om toe te voegen aan de channels naar de cores.

Het heeft de voorkeur om netwerkswitches met een dual power supply in te zetten, bij voorkeur intern gezien de beschikbare ruimte in de kast.

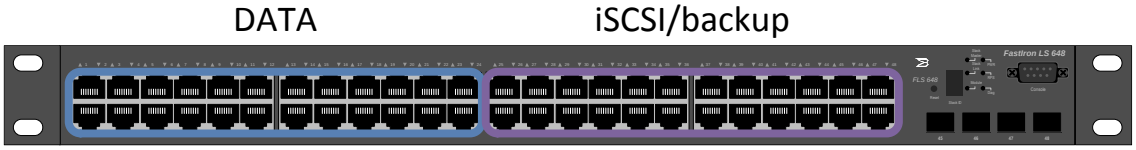
Schaalbaarheid: Om meer verbindingen of meer bandbreedte te kunnen faciliteren kunnen nieuwe switches in de stack worden bijgeplaatst.

Robuustheid: Bij uitval van een switch blijft de rest van de switch stack functioneren. Redundant gekoppelde systemen blijven functioneren.

Beheerbaarheid: Door het gebruiken van standaard configuraties voor het koppelen van nieuwe klanten en diensten wordt het beheer sterk vereenvoudigd.

Beveiliging: Management toegang is alleen mogelijk vanaf het netwerk management segment. Verkeer van de verschillende klanten is op vlan basis van elkaar gescheiden

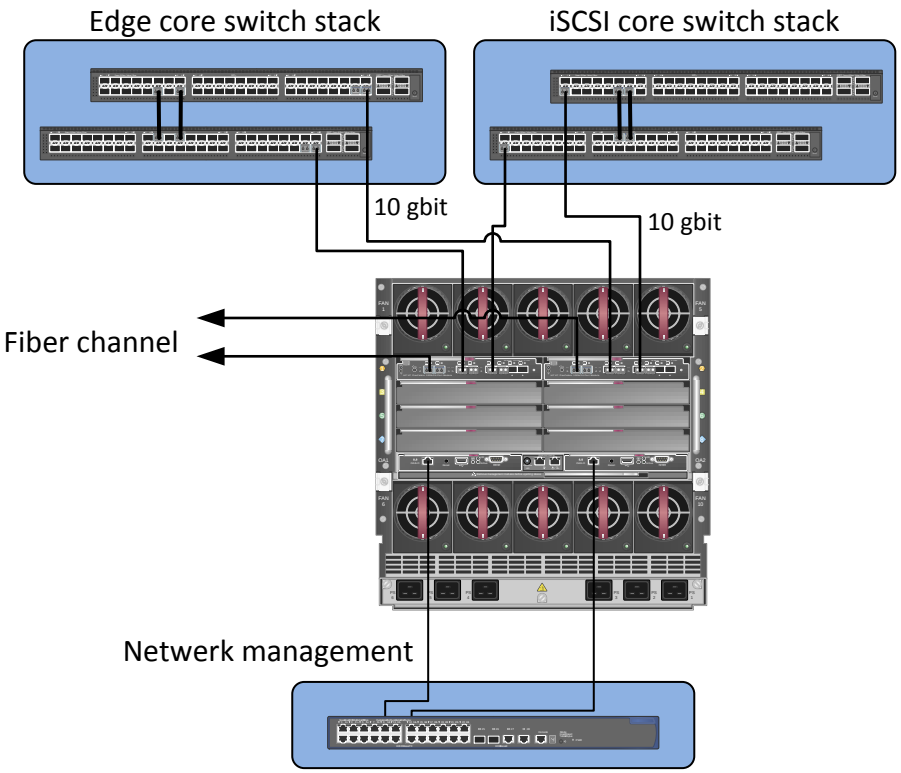
Een mogelijk poortindeling voor de Top of Rack switches is gegeven in Figuur 19



Figuur 19 Mogelijk indeling voor Top of Rack switches.

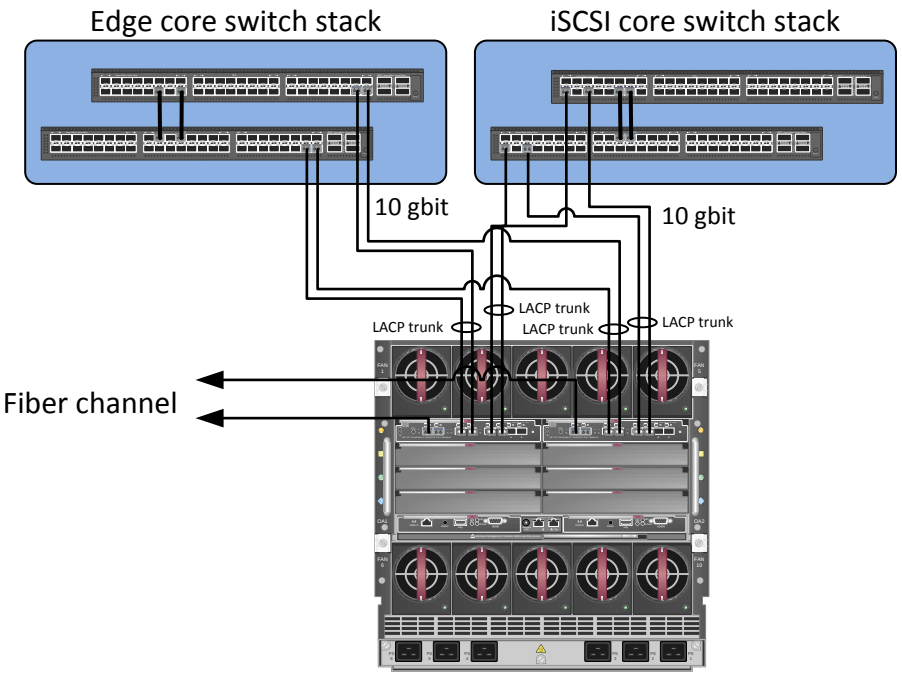
5.8.2. Blade enclosures

Blade enclosures worden direct op de Edge switch core gekoppeld. Onderstaande figuur geeft de details van de koppeling aan bij gebruik van een Virtual Connect FlexFabrix module.



Figuur 20 Details van de koppeling van enclosures op het netwerk.

De standaard configuratie voor de koppeling van een enclosure is een active-standby opzet.Wanneer er twee 10-gigabit links naar een core worden getrokken is de effectieve capaciteit dus 10 gigabit, slechts een van de links is tegelijk actief.



Figuur 21 Uitbreiding link capaciteit met LACP trunks.

Uitbreiding van de capaciteit kan eenvoudig door een LACP links te creeren naar zowel de edge als de iSCSI cores. Figuur 21 laat dit zien.

Onboard administrator poorten worden in de kast op de management switch gepatcht.

5.8.3. Servers

Servers worden op de Top of Rack switches gekoppeld. De Top of Rack switches hebben een sectie met data network poorten en een sectie met iSCSI poorten. De iSCSI en backup NIC worden gepatcht op de iSCSI sectie. De Datanetwerkpoorten worden gepatcht op de dat sectie. De ILO poort wordt gekoppeld op de netwerkmanagement switch.

5.8.4. iSCSI

Een groot deel van de storage bevindt zich op Lefthand iSCSI systemen.Voor iSCSI is het van belang dat het netwerk low-latency is en dat netwerkpoorten voorzien zijn van grote buffers. Het is sterk aan te bevelen om switches te gebruiken die geoptimaliseerd zijn voor iSCSI gebruik.

MTU size op de switches voor iSCSI is bij voorkeur zo groot mogelijk (9000 bytes) om de overhead zo laag mogelijk te houden. De werkelijk gebruikte MTU size is echter afhankelijk van de endpoints.

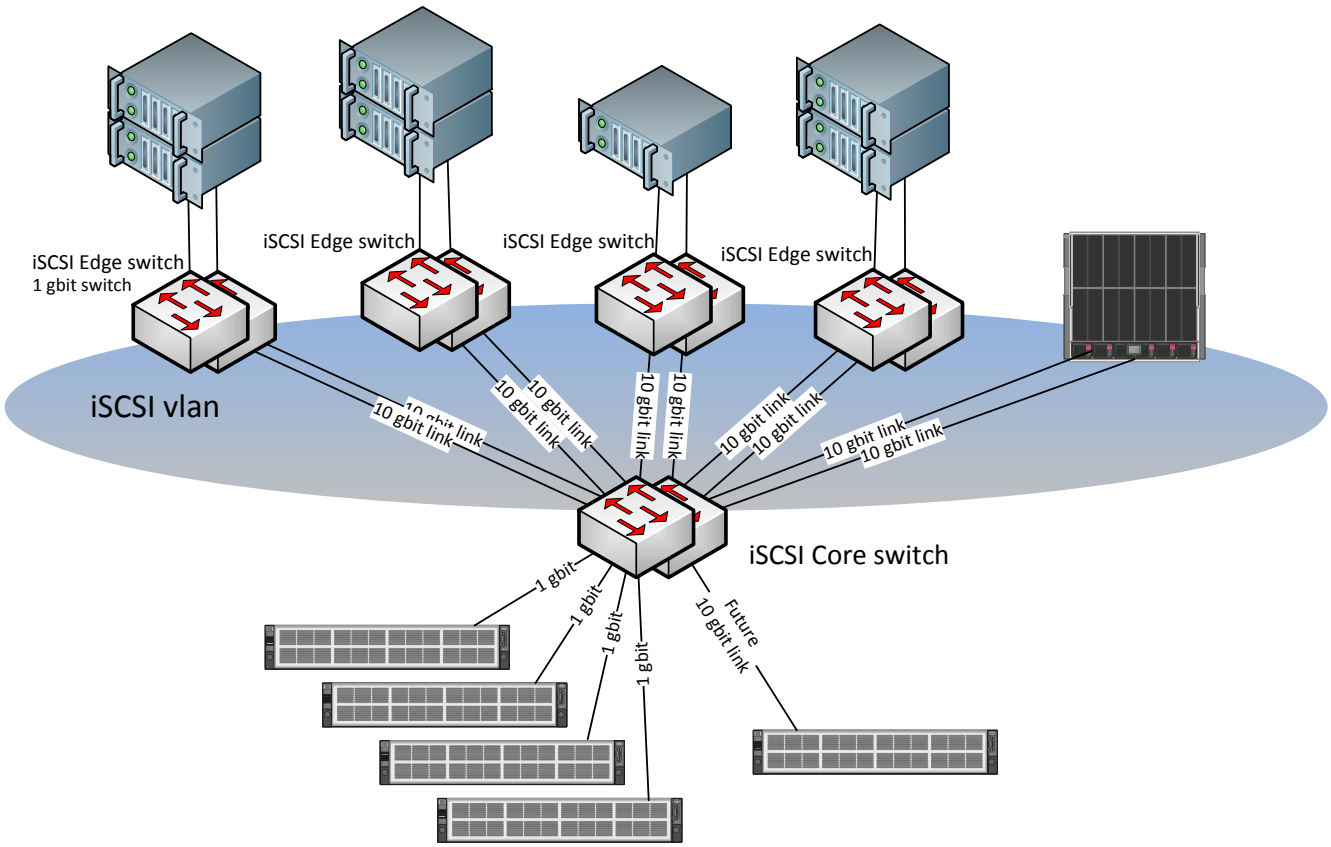


Figure 1 iSCSI netwerk design.

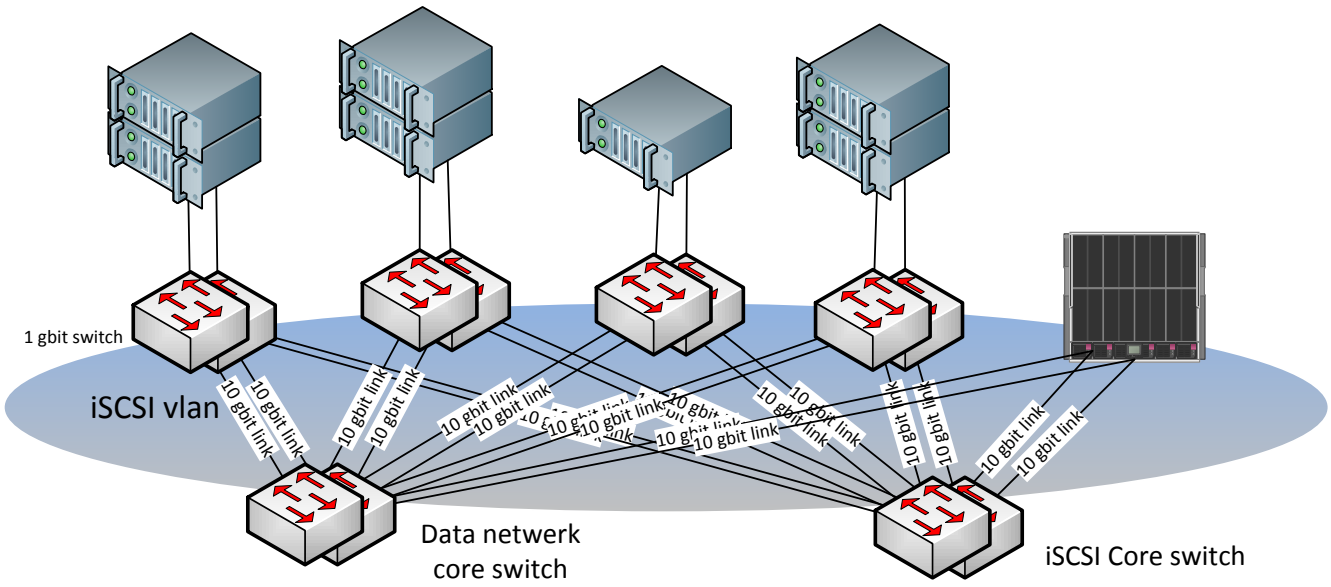
Om oversubscription te vermijden worden de iSCSI switches met 10 Gbit links gekoppeld naar de iSCSI core switch. Met een effectieve link capaciteit van 20 Gbit naar de core kunnen 20 1 Gbit iSCSI interfaces worden gebruikt per kast voordat oversubscription optreedt. De iSCSI core switch is een 10 Gbit switch waarop zowel 1 Gbit als 10 Gbit Storage systemen aan gekoppeld kunnen worden. Analoog aan de datnetwork core worden eventuele enclosures rechtstreeks met 10 Gbit gekoppeld op de iSCSI core.

De 10 Gbit iSCSI core maakt het mogelijk om de storage systemen in de toekomst te koppelen op 10 Gbit. Upgrade kits naar 10 Gbit zijn beschikbaar voor P4000 systemen.

De vrije rack ruimte is te beperkt om dedicated iSCSI switches in elk rack te gebruiken. Om het aantal switches te beperken wordt een iSCSI switch ook als data switch gebruikt maar heeft aparte uplinks naar de data center en iSCSI core.

Zowel de iSCSI Edge switch als de iSCSI Core switch zijn geclusterde switches waarbij de links tussen edge en core active-active gebruikt worden. Switchpoorten op de edge of de core uitbreiden kan door een extra switch aan de core toe te voegen.

Voor optimale performance worden jumbo frames en flow control gebruikt.



Figuur 22 Combinatie van data netwerk en iSCSI netwerk op de edge switches.

Op iedere edge switch set wordt een aantal poorten voor iSCSI gebruik gereserveerd.Het iSCSI vlan is niet gerouteerd en is een private vlan. Alle servers en enclosures zitten op private poorten om communicatie tussen systemen over de iSCSI poort onmogelijk te maken. Alleen de storage systemen zijn gekoppeld op "normale" poorten.

Bij gebruik van private vlans is het van belang dat zowel de fysieke als de virtuele switch private vlans ondersteunen. Vmware ondersteunt private vlans vanaf ESX 4.0.[1]

Schaalbaarheid: Om meer verbindingen of meer bandbreedte te kunnen faciliteren kunnen nieuwe switches in de stack worden bijgeplaatst.

Robuustheid: Bij uitval van een switch blijft de rest van de switch stack functioneren.Redundant gekoppelde systemen blijven functioneren.

Beheerbaarheid: Door het gebruiken van standaard configuraties voor het koppelen van nieuwe klanten en diensten wordt het beheer sterk vereenvoudigd.

Beveiliging: Management toegang is alleen mogelijk vanaf het netwerk management segment. De scheiding tussen tenants wordt hier gewaarborgd door het private vlan.

5.8.5. Backup netwerk

Het backup netwerk kan eveneens gebruik maken van de iSCSI infrastructuur. Het backup systeem wordt als een storage systeem gekoppeld op de iSCSI core switches. De backup nics van de servers worden op de iSCSI edge NICs gekoppeld. Voor het backup netwerk wordt een apart vlan met aparte gereserveerde poorten op de edge switches gecreeerd.

[1] VMware Knowledge base artikel 1010691

5.8.6. Management netwerk

Uit beheeroogpunt is het zeer aan te raden een losstaand management netwerk te hebben mede met het oog op beveiliging en het feit dat beide data centers "lights off" zijn. Het netwerk hoeft niet dubbel uitgevoerd te zijn omdat een failure gevolgen heeft voor de monitoring maar niet onmiddellijk een productieverstoring veroorzaakt. In de situatie bij de PRH data centers heeft een los management netwerk met een management switch in elke kast de volgende voordelen:

1. Het aansluiten van de huidige ILO en andere management poorten maakt onmiddelijk een aantal patches vrij op de patchpanelen in de kast en vereenvoudigt de migratie.
2. Het gebruik van goedkopere switches maakt de kosten per management poort flink lager, vaak is er sprake van een verlaging in de orde van 80%.
3. Goedkopere switches zijn ook kleiner en ondieper. Een managementswitch kan bovenin een datakast op dezelfde hoogte als een patchpaneel worden geplaatst.
4. Een losstaand out-of-band management netwerk is inherent veiliger dan een in-band management netwerk.

Als extra optie kunnen in de netwerkkasten routers als seriële terminalservers worden opgehangen. Deze kunnen via de patchpanelen worden gepatcht naar de verschillende Top of Rack en Core switches en ervoor zorgen dat deze switches ten allen tijde remote bereikbaar zijn.

Schaalbaarheid: Om meer te kunnen faciliteren kunnen nieuwe switches worden bijgeplaatst.

Robuustheid: Het management netwerk is enkel uitgevoerd.

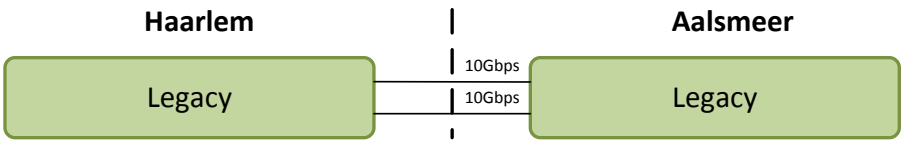
Beheerbaarheid: De opzet van het management netwerk is zeer eenvoudig. Beheerhandelingen zijn alleen nodig bij het toevoegen van apparatuur.

Beveiliging: Toegang tot het netwerkmanagement segment loopt via een firewall en een IPS. Daarnaast zijn de aangesloten systemen zelf nog beveiligd.

5.9. Inter-site verbindingen (ADVA)

Een ADVA FSP3000 Optical Transport wordt gebruikt voor de verbindingen tussen de data centers voor zowel data als iSCSI storage. De FSP3000 wordt ook gebruikt voor niet-iSCSI storage verbindingen maar dat valt buiten dit verhaal.

Figuur 23 geeft de huidige data en iSCSI inter-site verbindingen weer.



Figuur 23 Huidige Intersite DWDM verbindingen

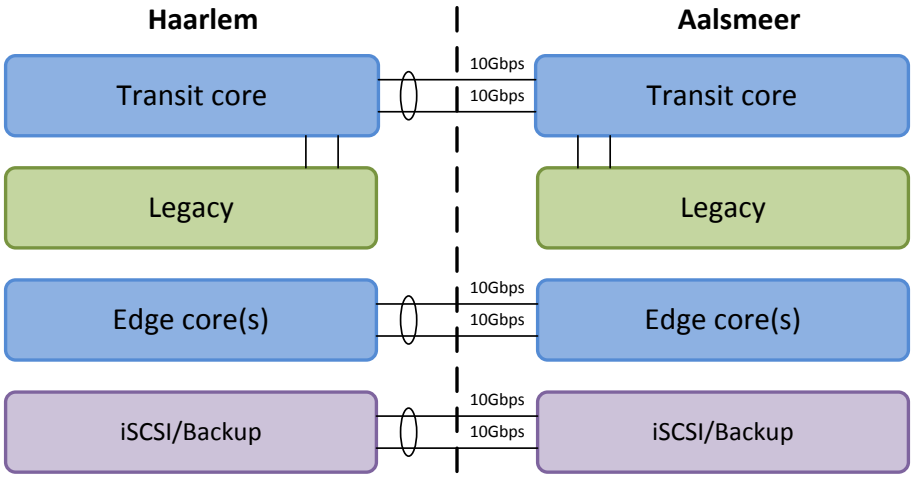
Om verkeersstromen goed te kunnen scheiden zijn 4 extra 10 Gbps verbindingen tussen de sites gewenst zoals gegeven in Figuur 24. De verbindingen tussen de locaties zijn channels van 2x10=20 Gbps per stuk. De Legacy omgeving maakt dmv Q-in-Q gebruik van de transportcapaciteit van de Transit core.

De Edge core maakt gebruik van een nieuw 20Gbps channel. Eventuele extra Edge cores kunnen met Q-in-Q ook getunneld worden door dit channel. Wanneer de capaciteit van dit channel

onvoldoende is om een nieuwe Edge core te hosten dan zullen de inter-site verbindingen opnieuw moeten worden uitgebreid.

Voor iSCSI wordt een apart channel gebruikt om interactie met het dataverkeer te vermijden.

Om deze channels te realiseren zijn twee extra 2-poorts 10 GBPS kaarten per FSP3000 nodig. Daarnaast zal waarschijnlijk een extra multiplexer module bijgeplaatst dienen te worden.



Figuur 24 Nieuwe inter-site verbindingen.

5.10. Vlan opzet

Bij aanwezigheid van een groot aantal klanten neemt ook het gebruik van vlans sterk toe. In één vlan domein passen maximaal 4096 vlans. De oplossing is dan om efficient om te gaan met vlans en om naar meerdere vlan domeinen toe te gaan.

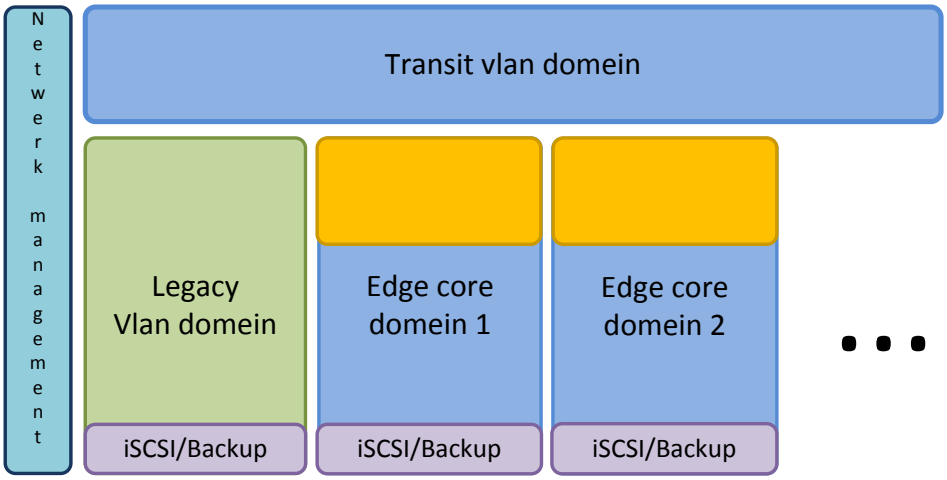
Dit ontwerp kent 4 vlan domeinen:

- De Transit core.
- De Legacy omgeving.
- De Edge core
- De netwerkmanagement omgeving (indien op eigen switches).

De Legacy omgeving staat volledig los van de nieuwe omgeving. In de nieuwe omgeving kan dus een nieuwe vlan structuur worden opgezet. Ook de Transit core en de Edge core zijn losse omgevingen. De tussenliggende firewall is echter gekoppeld aan beide vlan domeinen, het gekozen type (interne) firewall moet onderscheid maken tussen vlans op verschillende interfaces.

De Edge core zal het grootste aantal vlans herbergen en het sterkst groeien. Wanneer uit wordt gegaan van gemiddeld 8 vlans per klant kunnen 500 klanten gehuisvest worden op een Edge core omgeving. Door een nieuwe Edge core naast de bestaande te plaatsen kunnen opnieuw 500 klanten worden gehuisvest. Deze extra Edge core omgeving vormt ook weer een apart vlan domein.

De vlans voor iSCSI/backup omgeving zijn zowel in de Legacy als in de verschillende Edge core omgevingen aanwezig en moeten dus uniek zijn. In de eerdere vlan plaatjes zijn vlan 4000 t/m 4096 gereserveerd voor iSCSI en backup.



Figuur 25 Vlan domeinen

De netwerkmanagement omgeving is bij gebruik van losse switches ook volledig losgekoppeld. Wanneer netwerk management ook via de Top of Rack switches loopt dan moet hiervoor een reservering worden opgenomen van enkele vlans in de verschillende Edge core vlan domeinen.

5.11. IP adressing

Binnen de nieuwe geisoleerde klant hosting areas en de verbinding van de klant naar deze area mogen overlappende adresranges gebruikt worden. Voor de koppeling vanuit de hosting area naar de andere omgevingen wordt geNAT op de firewall. Op de transit core, de legacy omgeving, de internetkoppeling en de common services segmenten mag echter geen overlap optreden.

5.12. MSTP

Op de nieuwe omgeving wordt geen gebruik gemaakt van Spanning Tree om load-balancing mogelijk te maken. MSTP wordt wel gebruikt, maar alleen om het netwerk te beschermen tegen loops. Er komen twee MSTP regions, een region op de transit core en een region op de Edge core. De regions worden gescheiden door routerende firewalls en staan dus niet met elkaar in contact. Eventuele extra Edge omgevingen krijgen ook hun eigen MSTP Region.

PVST+ blijft gehandhaaft in zijn huidige vorm op de Legacy omgeving maar zal ook nergens raken aan de nieuwe MSTP regions.

5.13. VRRP

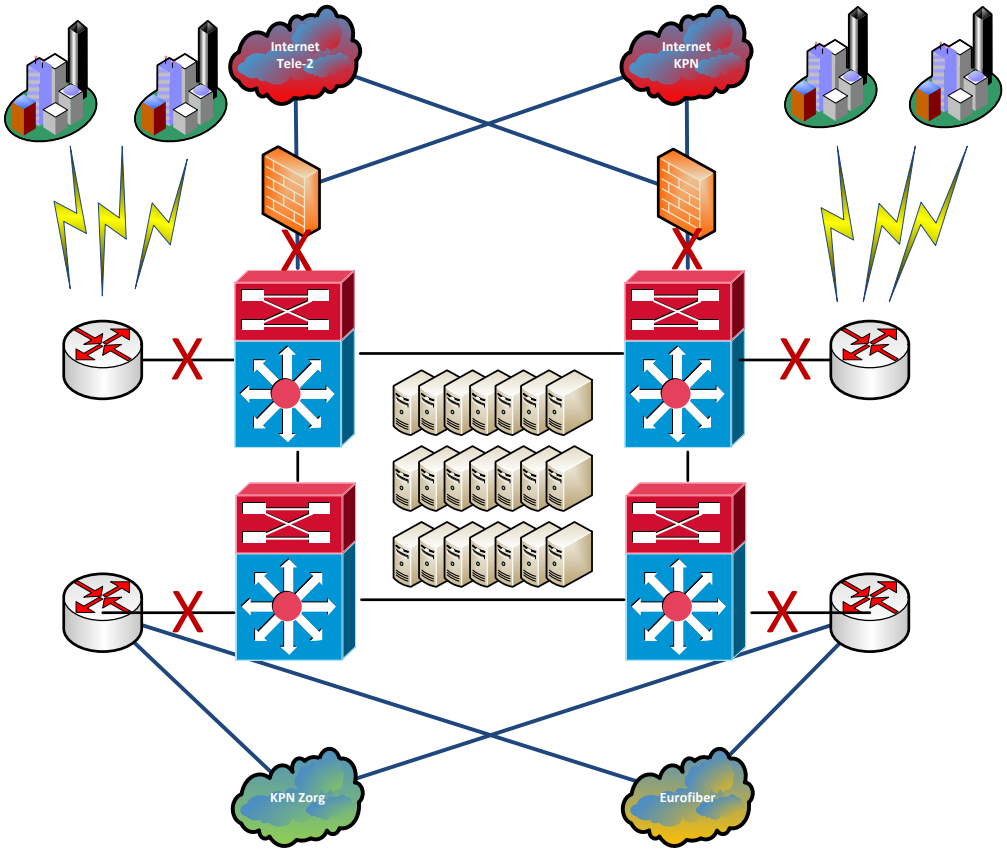
De default gateway op ieder subnet is redundant door het gebruik van de HA faciliteit van de firewall indien IP/MAC failover ondersteunt. Zo niet dan wordt redundancy gerealiseerd door het Virtual Router Redundancy Protocol (VRRP) .

6. Migratie

Ondanks dat migratie geen onderdeel van dit ontwerp is is er toch rekening mee gehouden. In dit hoofdstuk wordt heel ruw geschetst hoe de bestaande omgeving een plaats kan krijgen in het nieuwe ontwerp om vervolgens gefaseerd te worden gemigreerd.

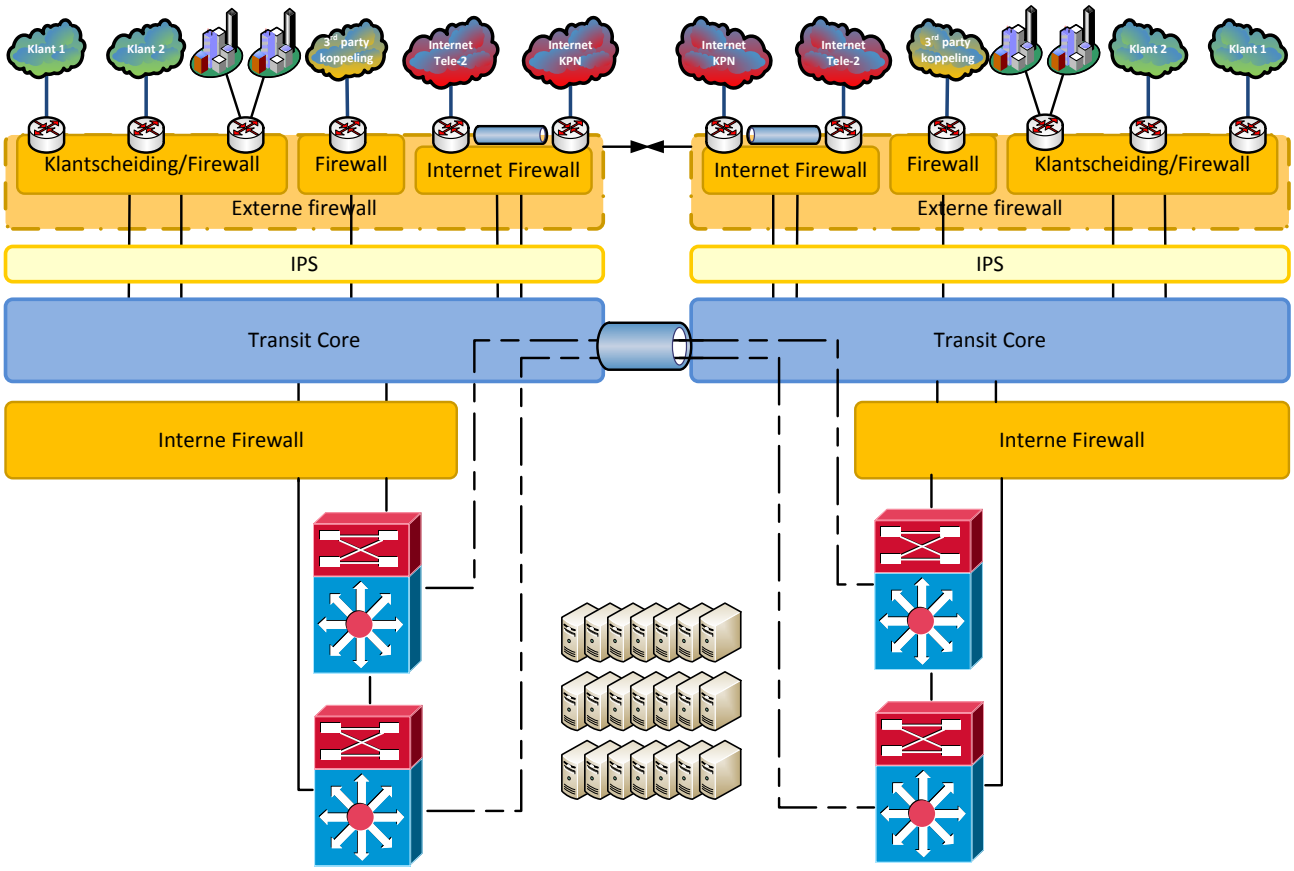
6.1. Inpassen van de Legacy omgeving

Het huidige netwerkplaatje bestaat uit een aantal WAN en internet routers gekoppeld aan een 10 gigabit ring rondom het datacenter. In het migratie scenario worden de WAN routers losgeknipt van de ring en met firewalls en IPSsen gekoppeld aan de nieuwe virtual backbone. De ring wordt vervolgens met firewalls gekoppeld aan dezelfde virtuele backbone.Op deze wijze wordt de bestaande omgeving direct beschermd door firewalls en IPS en wordt deze zodanig losgekoppeld van de nieuwe infrastructuur dat de nieuwe infrastructuur een nieuwe vlan opzet kan gebruiken onafhankelijk van de bestaande omgeving.



Figuur 26 Grove weergave van de Legacy omgeving voor de migratie.

Figuur 26 geeft een grove weergave van de huidige omgeving. De rode X–en geven aan waar de omgeving geknipt wordt.



Figuur 27 Legacy omgeving na de migratie.

Binnen het Legacy segment blijven de bestaande protocollen, PVST+ voor spanning tree en OSPF voor routering gehandhaaft. De bestaande OSPF area 6600 wordt via de firewall gekoppeld aan OSPF area 0 op de Transit core.

De Aalsmeer Legacy omgeving en de Haarlem Legacy omgeving worden via een Q-in-Q tunnel gekoppeld.

6.2. Kasten en apparatuur

Een van de requirements is dat de nieuwe apparatuur kan worden bijgeplaatst in de kasten en voor zover mogelijk gebruik maakt van de huidige bekabeling. Deze eisen hebben gevolgen voor het type apparatuur.

In de netwerkkasten is beperkt ruimte. Er is daarom gekozen voor firewall appliances en fixed port switches in plaats van modulaire switches waarin firewall blades kunnen worden geplaatst. Deze laatste zijn over het algemeen fors groter en kunnen niet zoals losse switches flexibel worden verdeeld over de beschikbare ruimte. Bijkomend voordeel van losse firewalls is dat de keuze van vendors breder is en losgekoppeld kan worden van de keuze voor de switch vendor.

Het verdient de voorkeur om voor de core switches 1U high density 10-gigabit switches te kiezen. In Haarlem is het waarschijnlijk nodig om enkele routers en of firewalls om te hangen naar

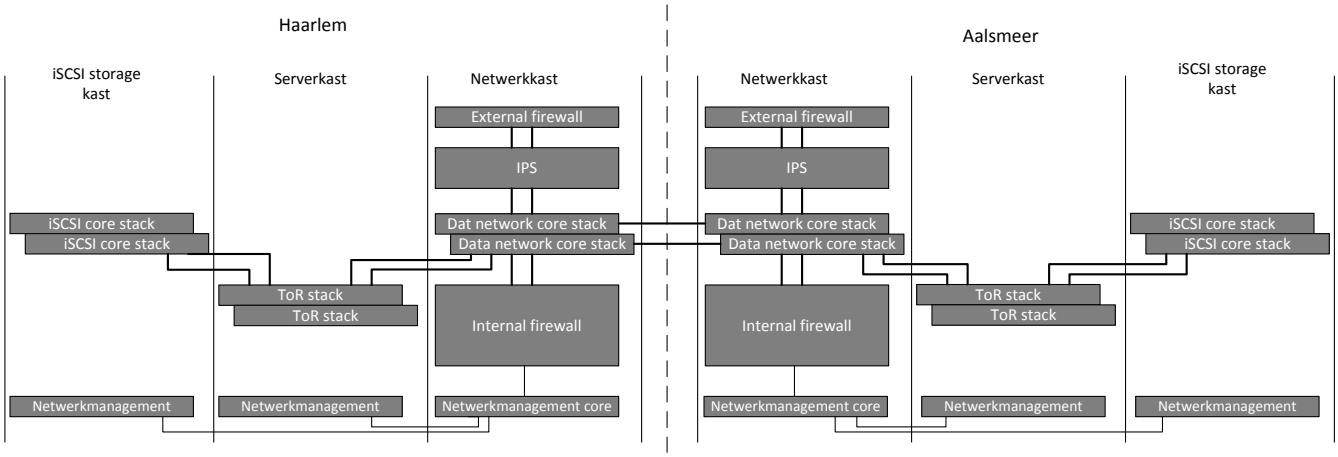
andere kasten om ruimte te scheppen voor de core switch stack. De meeste ruimte nemen de firewalls in. Afhankelijk van de keuze van de firewall zijn er één of twee per locatie nodig.

In de serverkasten worden Top of Rack switches gebruikt. Ook hier weer bij voorkeur 1U modellen. Per switch stack zijn er 2 glas uplinks naar de netwerkkast en 2 glas uplinks naar de iSCSI kast noodzakelijk. Per enclosure zijn er 4 glas uplinks nodig, eveneens 2 naar de netwerkkast en 2 naar de iSCSI kast. Eventuele Fiber Channel verbindingen zijn buiten beschouwing gelaten.

In de kasten met de iSCSI storage systemen worden de cores voor het iSCSI netwerk opgehangen, opnieuw met een voorkeur voor 1U modellen. iSCSI storage boxen in andere kasten kunnen hier via de bestaande patchpanelen met 1 gigabit UTP bekabeling op worden aangesloten. Gezien het grote aantal glasverbindingen naar de iSCSI core zal het nodig zijn om extra fiber bekabeling aan te leggen van de serverkasten naar het rack met de iSCSI core switches.

6.3. Fysieke plaatje

Met het design zoals beschreven in hoofdstuk 5 kan het uiteindelijke fysieke plaatje er als volgt uitzien:



Figuur 28 Overzicht fysieke componenten.

De core switches zijn 10 gigabit stacked switches met support voor contexten. Alle routering vindt plaats op de interne firewall. Schaalbaarheid wordt gerealiseerd door switches bij te plaatsen in de betreffende stack en door IPSsen of firewalls parallel te plaatsen.

Appendix A Kitlist

Om dit design te realiseren voor de twee locaties is het volgende nodig. Staat voor het aantal kasten dat van Top-of-Rack switches wordt voorzien.

Onderdeel	Aantal	Opmerkingen
48-poorts 10-gigabit switch	4	Core switch voor zowel transit als edge core. Ondersteunt contexten en is stackable
24 of 48-poorts gigabit switch	44	Top of Rack switch, extra grote poortbuffers voor iSCSI verkeer. Stackable. Uitgaande van 22 (12 in Aalsmeer en 10 in Haarlem) kasten die een Top-of-Rack switch nodig hebben
48- ports 10 gigabit switch	4	Core switch voor iSCSI en backup verkeer, extra grote poortbuffers voor iSCSI verkeer. Stackable.
RJ45 SFP mmodules	2x	Nodig voor aansluiten gigabit Lefthand storage of de iSCSI core uitgaande van x Lefthand storage boxen en 2 gigabit links per box.
24-poorts netwerk-management switch	26	Management switch per kast. Mag een 24-poorts 100 mbit model zijn. Kan eventueel hergebruikt zijn indien PRH al geschikte switches bezit.
48 poorts core netwerk-management switch	2	Centrale ‘core’ netwerkmanagement switch. Mag ook een stack van 2x24 poorts switches zijn. Ondiep model zodat weinig kastruimte vereist is.Kan eventueel hergebruikt zijn indien PRH al geschikte switches bezit.
Externe firewall	2	Deze firewall dient ook als VPN concentrator te kunnen functioneren. Eevntueel SSL offloading?
Interne firewall	2	Dit is een high speed low-latency firewall die clustering op basis van IP/Mac failover ondersteunt en een groot aantal contexten ondersteunt.
IPS	2	Een per site, capaciteit 2Gbps per stuk indien beschikbaar voorzien van een Zero Power High availabilty of equivalente voorziening.

De bestaande 7200 routers kunnen voorlopig gebruikt worden voor de internetkoppelingen. Wanneer BGP gebruikt gaat worden dan zijn de 7200VXR NPE-G2 routers voldoende om vol BGP internet routing toe te passen.

De opstapswitches zijn technisch eveneens voldoende om in het nieuwe ontwerp de eerste koppeling naar de klant locaties te blijven verzorgen. Standaardisatie van netwerkapparatuur in het data center kan echter een reden zijn om hier ook nieuwe switches voor te nemen.