ADVIES RAPPORT

IMPLEMENTATIE VAN IPV6 BINNEN TJIP

Datum:	7 juni 2011
Status:	Definitief
Versie:	1.01s
Project:	IPv6 voor meer ruimte
Opdrachtgever:	TJIP
Auteur:	Paul de Laat
Document:	aff.012.adviesrapport v1.01_s.docx

INHOUDSOPGAVE

1 INLEIDING

In dit document wordt beschreven hoe IPv6 binnen TJIP geïmplementeerd kan worden. Het document is gemaakt voor het afstudeeronderzoek van Paul de Laat. Het onderzoek wordt uitgevoerd in opdracht van TJIP en zal worden beoordeeld door de bedrijfsbegeleider van TIJP en afgevaardigde van de Fontys hogescholen te Eindhoven.

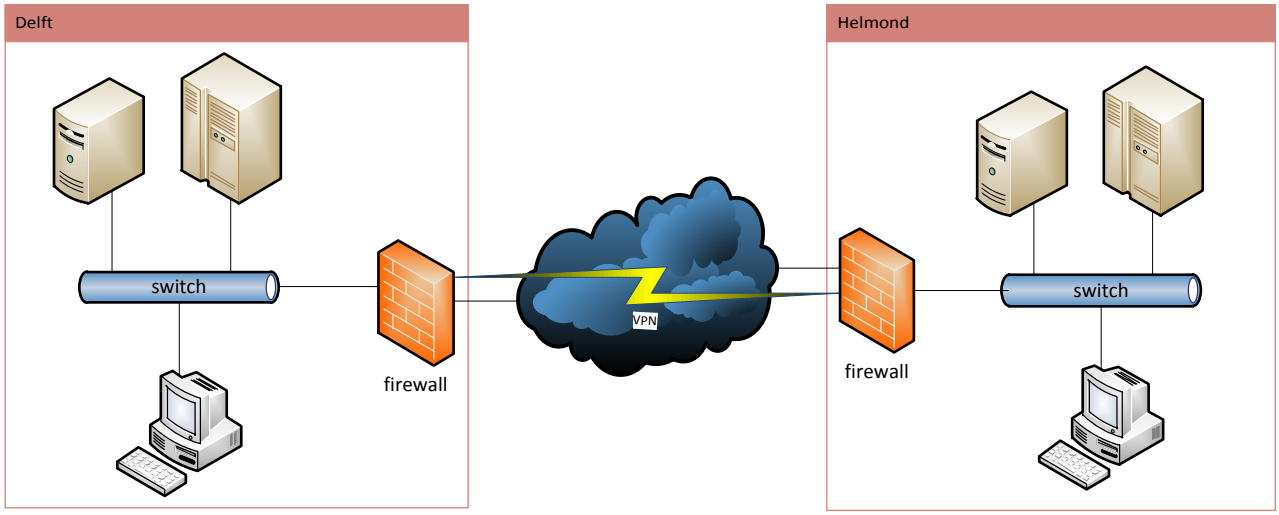
Er zal worden ingegaan op de inrichting van het netwerk, welke IP-adressen er gebruikt zullen worden en hoe de verbinding tussen de netwerken zal verlopen. Ook wordt er ingegaan op de configuratie van de systemen die in het netwerk aanwezig zijn en wordt de beveiliging van het netwerk besproken.

2 NETWERK

Voordat wordt begonnen met de implementatie van IPv6 dient er een helder beeld te zijn van de infrastructuur zoals die nu bij TJIP in gebruik is en hoe het er na de implementatie van IPv6 uit gaat zien. In dit hoofdstuk worden de bestaande en de nieuwe structuur van het TJIP netwerk gegeven. Hierin zullen de grootste wijzigingen worden besproken.

2.1 BESTAANDE NETWERKINDELING

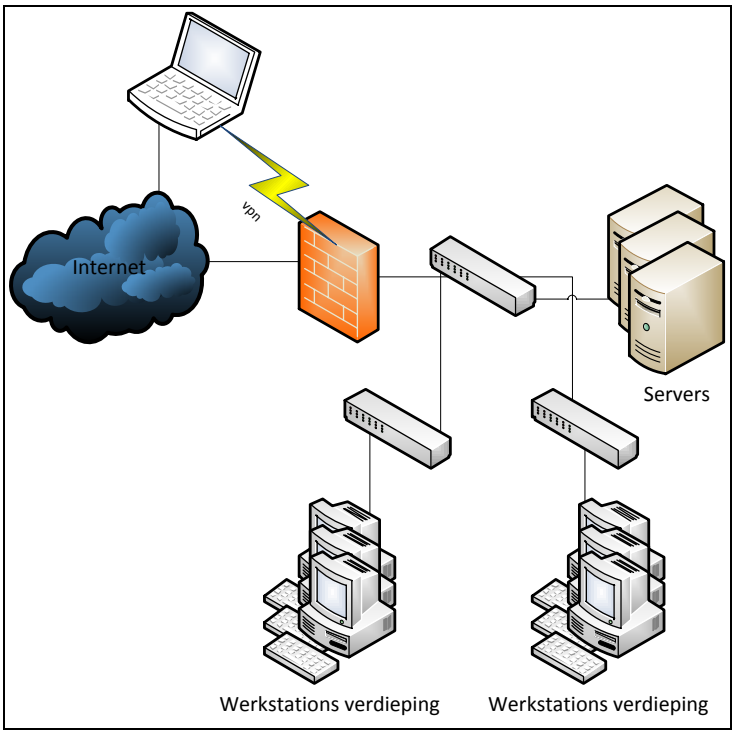
Het huidige netwerk van TJIP bestaat uit twee gedeeltes. Zo is er een netwerk op de locatie in Delft en een netwerk op de locatie in Helmond. Deze netwerken zijn met elkaar verbonden door middel van een vpn-verbinding over het internet. De vpn-verbinding wordt tot stand gebracht door de firewalls die in beide netwerken aanwezig zijn. In figuur 2.1 is dit vereenvoudigd weergegeven.



Figuur 2.1

Om de werkplekken van de medewerkers te voorzien van netwerktoegang zijn op de kamers netwerkaansluitingen aanwezig. Deze aansluitingen komen in de patchkast bij elkaar waar ze op verschillende switches worden aangesloten. Elke switch is weer verbonden met de backbone waarop ook de servers zijn aangesloten.

Voor medewerkers die van buiten kantoor verbinding willen maken met het TJIP netwerk is er de mogelijkheid om een vpn-verbinding te maken. Dit gebeurd met de vpn-client software die met de firewall wordt meegeleverd. In figuur 2.2 is dit vereenvoudigd weergegeven.

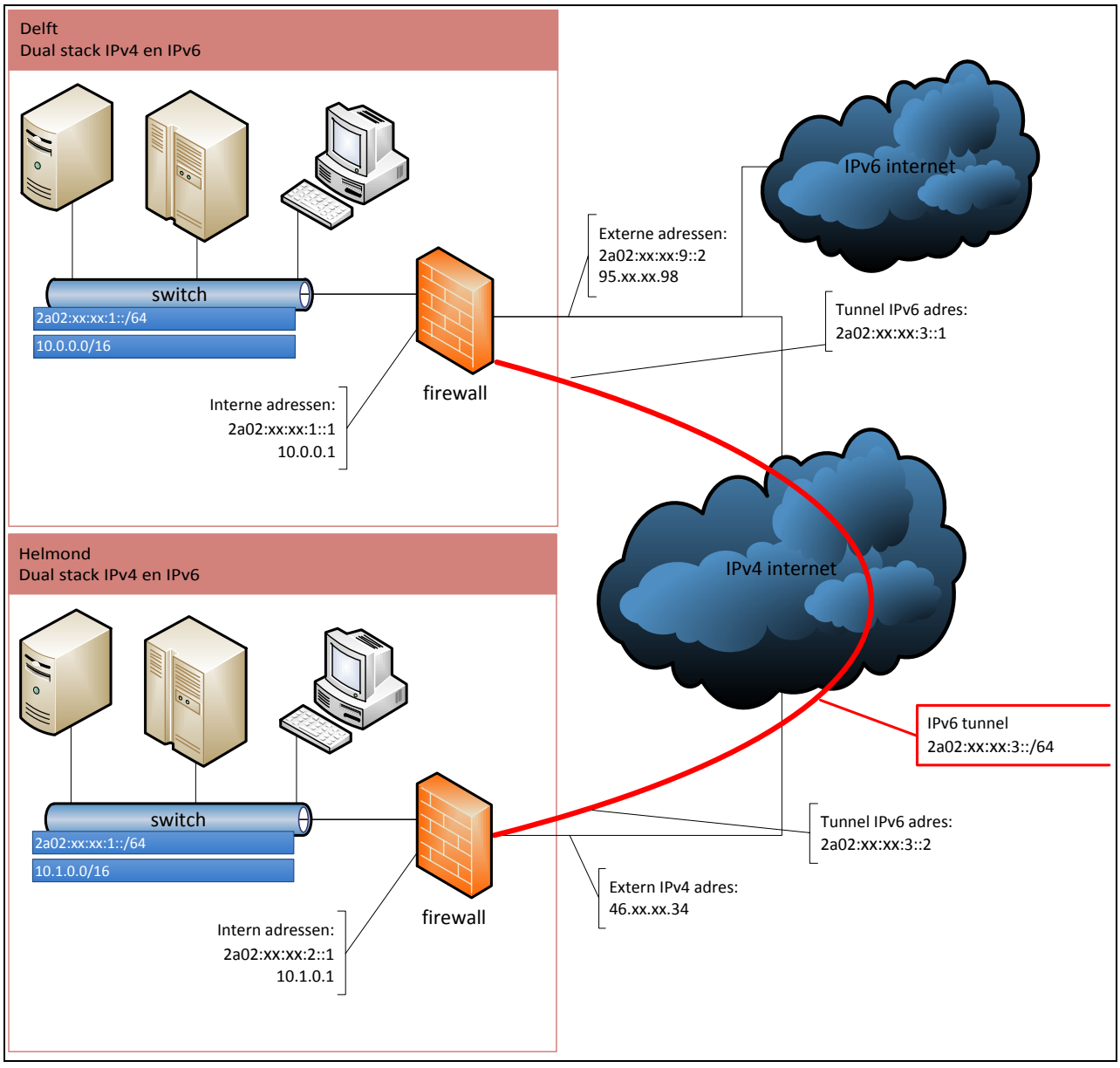


Figuur 2.2

2.2 INRICHTING VAN HET NIEUWE NETWERK

Wanneer IPv6 wordt geïmplementeerd blijft de huidige structuur en inrichting van het IPv4 netwerk behouden. Voor de implementatie van IPv6 zal er dus een laag over het IPv4 netwerk worden gelegd.

In Delft is de mogelijkheid om het netwerk direct op het IPv6 internet aan te sluiten. Dit wordt in de firewall geconfigureerd. Voor Helmond geld dat hier niet de mogelijkheid is om het netwerk direct op het IPv6 internet aan te sluiten. Om het netwerk in Helmond te voorzien van IPv6 connectiviteit zal er een IPv6 tunnel worden opgezet over het IPv4 internet naar het netwerk in Delft. In figuur 2.3 is dit vereenvoudigd weergegeven.



Figuur 2.3 Inrichting van het IP netwerk bij TIJP

Het opzetten van een IPv6 tunnel tussen de twee netwerken brengt met zich mee dat al het IPv6 verkeer van Helmond over deze tunnel naar Delft gaat om vanuit daar het internet op te gaan. Ook IPv6 verkeer voor de locaties Delft en Helmond onderling zal over de tunnel worden verstuurd. Het netwerkverkeer dat door een IPv6 tunnel wordt gestuurd is standaard niet versleuteld. Om te voorkomen dat interne data onversleuteld over de IPv6 tunnel gaat dient er

een VPN tunnel hier omheen geconfigureerd te worden voor het interne IPv6 verkeer tussen de vestigingen.

Wanneer het netwerk in Helmond zelf kan beschikken over IPv6 connectiviteit is de noodzaak van de tunnel niet meer aanwezig. De tunnel kan dan tussen de twee netwerken worden verwijderd. En de VPN tunnel kan dan over het IPv6 internet worden gestuurd.

3 IPV6 NETWERK

Om binnen TJIP een werkend IPv6 netwerk te krijgen is het van belang dat een aantal netwerk services worden geüpgrade. Zoals aangegeven in het onderzoeksverslag zijn de router / firewall, de DHCP en de DNS service niet geschikt om IPv6 te verwerken. In dit hoofdstuk zal kort besproken worden hoe dit opgelost kan worden en waarmee rekening gehouden dient te worden bij de upgrade van de systemen.

3.1 ROUTER / FIREWALL

De huidige router / firewall oplossing die binnen TJIP wordt gebruikt (Kerio Control 7.1.2) bied geen ondersteuning voor IPv6. Om IPv6 connectiviteit te verkrijgen is het noodzakelijk dat er een router / firewall oplossing wordt gebruikt die IPv6 wel ondersteund.

Voor het opzetten van de proof of concept omgeving is gebruik gemaakt van de oplossing van Vyatta. Er is gebruik gemaakt van de Vyatta 6.2 virtual appliance die als virtual machine draait op een ESXi 4.1 server. Vyatta is open source router software. Het is een erg krachtige oplossing met veel mogelijkheden en instellingsmogelijkheden. Het is mogelijk om Vyatta op op twee manieren te configureren. Er is een command line interface en een web interface om Vyatta te configureren en te beheren.

Het nadeel van Vyatta is dat er niet gemakkelijk een overzicht te krijgen is van de verschillende instellingen. Bij andere systemen is het vaak zo dat bijvoorbeeld firewall instellingen onder elkaar staan. Hierdoor kan er snel een beeld worden verkregen over de verschillende instellingen waardoor risico's snel gezien kunnen worden.

3.1.1 NETWERK

Het netwerk in Delft kan door de internet provider van IPv6 connectiviteit worden voorzien. Hiervoor heeft TJIP van de provider onderstaande gegevens ontvangen.

> ***Buitenkant van firewall bij TJIP:***
>
> *IP-adres voor de router 2a02:xx:xx:xx::2 /64 (dit is het adres waar het /48 blok naar toe wordt gerouteerd, er kan geen ander adres worden toegepast).*
>
> *gateway 2a02:xx:xx:xx::1*
>
> ***Binnenkant firewall TJIP:***
>
> *IPv6 reeks voor TJIP 2a02:xx:xx::/48*
>
> *Bijvoorbeeld: Interne IP-adres van de router: 2a02:xx:xx:1::1/64*
>
> *(Deze gegevens zijn op maandag 9 mei 2011 ontvangen van Paul Hoogsteder van Breedband Delft)*

Om het netwerk van TJIP in Delft te voorzien van IPv6 adressen wordt er gebruikgemaakt van het subnet 2a02:xx:xx:1::/64. Hieruit krijgt de gateway het IP-adres 2a02:xx:xx:1::1 toegewezen. Alle andere systemen uit het netwerk zullen zelf een IP-adres genereren op basis van het subnet.

Voor het netwerk in Helmond wordt het subnet 2a02:xx:xx:2::/64 gebruikt. Ook uit dit subnet zal het eerste IP-adres, 2a02:xx:xx:2::1, aan de router worden toegekend.

Voor de IPv6 tunnel wordt gebruikgemaakt van een derde subnet, te weten 2a02:xx:xx:3::/64. Hieruit wordt eerste IP-adres gebruikt voor de router in Delft en tweede voor de router in Helmond.

Router Delft

- Externe interface: 2a02:xx:xx:xx::2 /64
- Interne interface: 2a02:xx:xx:1::1/64
- IPv6 tunnel: 2a02:xx:xx:3::2/64

Router Helmond

- Externe interface: geen IPv6 beschikbaar
- Interne interface: 2a02:xx:xx:2::1/64
- IPv6 tunnel: 2a02:xx:xx:3::2/64

In figuur 2.3 is de verdeling van de subnetten en IP-adressen al een keer grafische weergegeven.

3.2 DHCP

De huidige DHCP services wordt gedraaid op een MS server 2003. MS server 2003 bied geen ondersteuning voor DHVPv6. Het is mogelijk om via een externe applicatie een DHCPv6 service op de server te installeren. Deze zal dan niet geïntegreerd zijn met de Active Directory en DNS server waardoor de voordelen van een DHCPv6 server niet worden gebruikt.

Het is mogelijk om de huidige servers te upgraden naar een versie die wel DHCPv6 ondersteund. Voor Microsoft servers geld dat er vanaf versie 2008 ondersteuning is voor DHCPv6. Wanneer een systeem wordt geüpgrade wordt geadviseerd om dan maar naar de nieuwste versie van de server omgeving (MS server 2008 R2) te upgraden.

De systemen upgraden levert een heleboel werk op en zal buiten kantooruren uitgevoerd dienen te worden omdat anders de productie binnen TJIP wordt gehinderd. Om dit te voorkomen kan er op beide locaties een nieuwe Domain controller worden ingericht. Hierop wordt een DHCPv6 service gedraaid. Op deze manier kan de productie gewoon doorgaan en kan op een gegeven moment de DHCP service op de huidige Domain controller worden gestopt en op de nieuwe server worden gestart.

3.3 DNS

Voor de DNS servers die nu binnen TJIP in gebruik zijn geld het zelfde als voor de DHCP servers. De huidige versies van de DNS servers ondersteunen IPv6 niet volledig. Er kunnen nu wel al AAAA-records worden toegevoegd in de DNS server, maar reverse lookup van IPv6 adressen wordt niet ondersteund.

Om IPv6 volledig te ondersteun wordt geadviseerd om ook de nieuwe versie van de DNS service te gaan gebruiken op een MS server 2008 R2 server. Deze service kan zonder problemen op het zelfde systeem draaien als de DHCP service.

De DNS services op de MS server 2003 systemen kan worden uitgeschakeld wanneer de DNS services op de nieuwe MS server 2008 R2 systemen zijn gesynchroniseerd met de bestaande DNS. Hiermee kan, zonder dat de gebruikers dit merken worden gemigreerd.

Zorg er wel voor de DHCP servers aan systemen in de twee netwerken het adres van de nieuwe DNS servers aan de clients geeft. Dit voordat de DNS service op de Server 2003 systemen wordt gestopt.

4 NODES

Binnen TJIP worden verschillende nodes binnen het netwerk gebruikt. De meeste zijn fysieke of virtuele systemen die zijn voorzien van een Microsoft besturingssysteem. Verder zijn in het netwerk een aantal systemen aanwezig die draaien met een Linux besturingssysteem. Ook zijn er een aantal apparaten die zijn voorzien van een fabrikant specifiek besturingssysteem.

Voor de implementatie van IPv6 hoeven niet alle systemen in het netwerk voorzien te worden van IPv6. Omdat er een Dual stack implementatie van IPv6 plaats zal vinden binnen het TIJP netwerk kunnen alle systemen elkaar nog steeds bereiken via IPv4. Als twee systemen in het netwerk met elkaar willen communiceren en beide beschikken ze over zowel IPv4 als IPv6 zal IPv6 worden gebruikt voor de communicatie.

Er bestaat bij TIJP vooral de behoefte om zelf IPv6 services te kunnen benaderen op het internet. Het bereikbaar maken van de eigen systemen op het IPv6 internet is van minder groot belang. Dit brengt met zich mee dat vooral de werkplekken van de medewerkers voorzien dienen te zijn van IPv6 connectiviteit en dat de verschillende server, die diensten aanbieden op het netwerk en het internet, niet perse voorzien hoeven te worden van IPv6 connectiviteit.

4.1 MICROSOFT SYSTEMEN

Zoals aangegeven zijn de meeste systemen binnen het netwerk van TJIP voorzien van een Microsoft besturingssysteem. Zo zijn de meeste werkplekken van gebruikers voorzien van Windows 7 en worden nieuwe servers voorzien van Server 2008 R2. Ook zijn er nog een heleboel virtuele en fysieke Windows XP systemen en Server 2003 servers aanwezig binnen TJIP.

Voor de Windows 7, Windows Vista, Server 2008 en Server 2008 R2 systemen geldt dat deze standaard IPv6 ondersteunen. Aan deze systemen hoeft niets veranderd te worden. Als er een IPv6 router in het netwerk wordt geplaatst zullen deze systemen automatisch de gegevens gaan gebruiken die de IPv6 router uitgeeft. Dit komt doordat het IPv6 protocol wordt geprefereerd boven het IPv4 protocol.

Voor oudere Microsoft besturingssystemen geld dat het IPv6 protocol standaard niet aan staat. Dit dient op alle systemen waarop IPv6 connectiviteit gewenst is handmatig aangezet te worden. Om gebruik te kunnen maken van een DHCPv6 server dienen de oudere besturingssystemen voorzien te worden van extra software.

Het gebruik van DHCPv6 op de oudere systemen is handig voor het terugzoeken van een naam bij een IP-adres. Maar het is niet noodzakelijk voor systemen. Doordat ze van de IPv4 DNS server ook de AAAA-records van een site krijgen hoeft er geen IPv6 DNS server opgegeven te worden om DNS te kunnen gebruiken. Als een netwerk alleen uit IPv6 bestaat dient er wel DHCPv6 gebruikt te worden omdat systemen anders niet weten waar de DNS server zich in het netwerk bevind.

4.2 LINUX SYSTEMEN

In het netwerk van TJIP zijn ook een paar Linux systemen aanwezig. De meeste hiervan zijn geïnstalleerd op netwerkapparaten (storage, printers). Afhankelijk van de kernel versie en de distributie is er in deze systemen ondersteuning voor IPv6. IPv6 is voor deze apparaten niet van belang. De diensten die erop draaien zijn alleen bedoeld voor intern gebruik.

De virtuele omgevingen van TJIP bestaan uit verschillende ESX en ESXi servers. ESX en ESXi zijn op Linux gebaseerde systemen die door de fabrikant, VMWare, zijn aangepast.

Vanaf versie 4.0 ondersteunt VMWare met ESX en ESXi IPv6. Hiervoor is deze ondersteuning nog niet aanwezig. Binnen TJIP zijn echter nog een aantal ESX 3.5 servers aanwezig. De virtuele systemen die draaien binnen ESX 3.5 kunnen gewoon gebruikmaken van IPv6. Dit verkeer wordt door de ESX server niet anders verwerkt dan IPv4 verkeer. Het is echter niet mogelijk om over IPv6 met de ESX server te communiceren.

Ook voor alle ESX servers geld dat het niet nodig is en zelfs ongewenst is als deze direct via het internet benaderd kunnen worden. Met IPv4 is dit nu niet het geval en als IPv6 wordt geïmplementeerd zullen de systemen ook niet vanaf het internet benaderd dienen te worden.

4.3 SYSTEMEN MET FABRIKANT SPECIFIEKE BESTURINGSSYSTEMEN

Voor de apparaten in het netwerk die beschikken over een fabrikant specifiek besturingssysteem geldt dat ze niet via het internet benaderd hoeven te worden. Hierdoor voldoet IPv4 nog prima en is er geen noodzaak om de systemen naar IPv6 te migreren.

Als steeds meer apparaten en systemen IPv6 gaan gebruiken neemt de noodzaak van IPv4 steeds meer af. Het zal nog wel een hele tijd duren voordat IPv4 helemaal niet meer gebruikt wordt, maar als je als bedrijf terug kan gaan van twee IP infrastructuren naar één infrastructuur scheelt dit in de configuratie en beheer van het netwerk. Om die overstap te kunnen zetten is het dan wel van belang dat alle apparaten binnen het netwerk het IPv6 protocol kunnen gebruiken.

Nu is het schrappen van IPv4 binnen de organisatie nog niet aan de orde omdat op internet de meeste diensten nog via IPv4 worden aangeboden en dit nog een hele tijd het meest gebruikte protocol blijft, maar dit zal geleidelijk minder worden en verdwijnen. Wanneer er dan binnen de organisatie nog systemen zijn die alleen IPv4 ondersteunen kan IPv4 niet worden uit gefaseerd. Door nu al bij de aanschaf van nieuwe apparatuur en software rekening te houden met IPv6 ondersteuning zal dit een uitfasering van IPv4 niet in de weg staan.

4.4 CONCLUSIE

De werkstations die door de medewerkers van TIJP worden gebruikt zijn geschikt om IPv6 te gebruiken. De meeste hiervan behoeven hiervoor geen enkele configuratie. Alleen op werkstations met Windows XP dient het IPv6 protocol geactiveerd te worden.

Voor de virtuele omgevingen is het niet noodzakelijk dat IPv6 hierop volledig ondersteund wordt. Het is voldoende dat IPv6 door de virtuele systemen kan worden gebruikt op alle ESX servers.

Als er geen nieuwe netwerk apparatuur wordt aangeschaft zonder ondersteuning voor IPv6 kan IPv4 in de toekomst sneller worden uit gefaseerd. Dit scheelt in de configuratie en het beheer van systemen en het netwerk.

5 BEVEILIGING IPV6 NETWERK

Omdat de beveiliging van data van cruciaal belang is voor een bedrijf, en dus ook voor TJIP, is dit ook bij IPv6 van belang. Door de implementatie van IPv6 binnen een organisatie wordt de kwetsbaarheid vergroot. Door via een extra protocol te gaan communiceren met de buitenwereld wordt het raakvlak van het interne netwerk met de buitenwereld als het ware vergroot.

Om te voorkomen dat de implementatie van IPv6 leid tot extra kwetsbaarheden is het nodig om goed in de gaten te houden hoe het gebruikt gaat worden en op welke manier het gebruikt gaat worden. In dit hoofdstuk wordt ingegaan op manieren om dit tegen te gaan.

5.1 BEREIKBARHEID

Anders dan bij de huidige IPv4 implementatie bij TJIP zullen met IPv6 alle systemen worden voorzien van een uniek routeerbaar IPv6 adres. Dit houdt in dat, wanneer er geen filter zou worden toegepast, de systemen vanaf het internet direct te benaderen zijn. Door op de firewall in te stellen dat er geen verkeer mag plaatsvinden naar systemen zonder dat hierom is gevraagd is dit direct te ondervangen.

Een goede firewall blokkeert standaard al het verkeer dat door de firewall heen wil komen. Door regels op te stellen over verkeer dat je wel wilt toestaan door de firewall heen bepaal je welke data het netwerk mag verlaten en op mag komen.

Voor TJIP zal het in eerste instantie zijn dat er geen diensten over IPv6 naar buiten zullen worden aangeboden. Door in de firewall in te stellen dat al het verkeer vanaf het interne netwerk naar buiten wordt toegestaan, kunnen systemen in het netwerk naar systemen buiten het netwerk data sturen.

Als een systeem vanaf het internet dan data terug stuurt zal dit worden geblokkeerd. Om dit verkeer toch toe te staan dient de firewall bij te houden vanaf welk intern adres naar welk extern adres data is verstuurd en het verkeer wat terug komt ook toe te staan. Dit kan in de firewall worden ingesteld.

Later zullen er ook diensten vanuit het interne netwerk worden aangeboden aan systemen op het internet. Hiervoor dient per dienst een regel aangemaakt te worden waarin wordt aangegeven naar welk IP-adres of welke IP-reeks data gestuurd mag worden en over welke poorten het dataverkeer is toegestaan.

De configuratie hiervan is vergelijkbaar met die van een IPv4 firewall, alleen is het niet nodig om de vertaling van externe IP-adressen en poorten naar interne IP-adressen en poorten uit te voeren.

5.2 SCANNING

Een IP-adres bestaat uit een netwerk gedeelte en een host gedeelte. Bij IPv4 is dit variabel. IPv4 netwerken kunnen een netwerkgedeelte van 1 tot en met 31 bits hebben. Echter de meest gebruikt lengtes zijn 8, 16 en 24 bits. In IPv6 netwerken kan de lengte van het netwerkgedeelte ook variëren, maar de laatste 64 bits behoren altijd tot het host gedeelte.

Doordat de laatste 64 bit van een IPv6 adres specifiek zijn voor een bepaalde host is het scannen van IP adressen erg veel werk. In de meeste IPv4 netwerken zijn alleen de laatste acht bits (/24 netwerk) verantwoordelijk voor het bepalen van een host. Binnen TJIP zijn dit de

laatste 16 bits (/16 netwerk). Wanneer er een netwerkscan wordt uitvoerd voor het IPv4 netwerk is een netwerksysteem hier ongeveer 10 minuten mee bezig.

In tabel 5.1 is voor de verschillende netwerkgroottes aangegeven hoeveel adressen de netwerken kunnen bevatten. De tijd die nodig is om het netwerk te scannen is recht evenredig met het aantal IP-adressen.

Tabel 5.1 Maximum aantal IP-adressen in een netwerk

	Netwerk gedeelte	Host gedeelte	Max. aantal adressen in het netwerk
IPv4 /24	24 bits	8 bits	256
IPv4 /16	16 bits	16 bits	65.536
IPv6 /64	64 bits	64 bits	18.446.744.073.709.551.616

Uit tabel 5.1 is te halen dat het doorzoeken van een compleet 64 bit IPv6 subnet $2{,}8*10^{14}$ keer zolang duurt als het doorzoeken van een 16 bit IPv4 adres. De snelheid van het doorzoeken is afhankelijk van de gebruikte apparatuur, methode en de snelheid van de verbindingen.

Als een snelle scan van het IPv4 /16 subnet nu 10 minuten duurt, zal een zelfde scan van een IPv6 /64 netwerk 5355307776 jaar duren.

Het in kaart brengen van een IPv6 netwerk wordt er voor hackers dus niet gemakkelijker op in vergelijking met een IPv4 netwerk.

5.3 NEIGHBOR DISCOVERY PROTOCOL

Als het scannen van het netwerk niet meer tot de opties behoord zullen de hackers een andere manier gaan zoeken om systemen in kaart te brengen. Dit kan door gebruik te maken van het Neighbor Discovery protocol.

Het ND protocol maakt gebruik van ICMP6 pakketten. Het op alle systemen blokkeren van ICMPv6 is echter geen optie omdat het dan voor systemen niet meer mogelijk is om IP-adressen te verkrijgen. Er zou gekozen kunnen worden om alle ICMP6 verkeer te accepteren van bepaalde systemen zoals de router en de DHCP server, maar dit gaat problemen opleveren met DAD (Duplicate Address Detection).

Er wordt gewerkt aan het SND protocol wat staat voor Secure Neighbor Discovery protocol, maar dit is nog volop in ontwikkeling en er is nog weinig over te vinden. Ook wordt het nog maar weinig ondersteund door besturingssystemen en apparaten.

5.4 IPV6 VERKEER TUSSEN DELFT EN HELMOND

Om IPv6 connectiviteit te krijgen tussen Delft en Helmond wordt er gebruik gemaakt van een tunnel tussen de twee locaties. Het verkeer in de tunnel is niet versleuteld en kan op het internet dan ook onderschept worden. Om te voorkomen dat het netwerkverkeer dat tussen de netwerken wordt verstuurd onversleuteld over het internet gaat dient de IPv6 tunnel door een VPN tunnel te worden geconfigureerd.

Wanneer de locatie in Helmond ook de beschikking krijgt over native IPv6 connectiviteit is de IPv6 tunnel niet meer nodig. Dit houdt echter niet in dat de VPN tunnel niet meer gebruikt dient te worden. Als de VPN tunnel niet meer wordt gebruikt worden de netwerkpakketen van Helmond naar Delft onversleuteld over het IPv6 internet verstuurd.

Om het verkeer veilig tussen de netwerken te kunnen versturen dient er dan een VPN tunnel geconfigureerd te worden voor het IPv6 verkeer. Dit zal een andere tunnel worden dan die voor het IPv4 verkeer omdat ze over twee verschillende netwerken gaan.

5.5 CONCLUSIE

Het beschermen van een IPv6 netwerk is niet ingewikkelder dan het beschermen van een IPv4 netwerk. Doordat NAT niet nodig is kan het configureren van de firewall zelf eenvoudiger zijn, er hoeft namelijk geen vertaling meer plaats te vinden van externe adressen naar interne adressen.

Een IPv6 netwerk in kaart brengen door middel van een netwerkscan is onbegonnen werk. Hiervoor dient een hacker gebruik te maken van het Neighbor Discovery protocol. Er wordt gewerkt aan een veiligere versie van dit protocol, maar dit wordt nu nog niet ondersteund door de systemen die bij TJIP in gebruik zijn.

Dat IPv6 in kaart kan worden gebracht met het Neighbor Discovery protocol wil niet zeggen dat dit protocol kwetsbaarder is dan IPv4. In een IPv4 netwerk kan met een netwerkscan een netwerk in kaart worden gebracht en dit is in een IPv6 netwerk weer niet te doen.

Een IPv6 tunnel tussen Helmond en Delft is niet voldoende om het netwerkverkeer vertrouwelijk tussen de vestigingen uit te kunnen wisselen. Hiervoor dient een IPv6 tunnel in een VPN tunnel geconfigureerd te worden.

6 CONCLUSIE

Voor de implementatie van IPv6 bij TJIP zullen er in Delft en Helmond nieuwe domain controllers worden geïnstalleerd die worden voorzien van DHCP, DHCP6 en DNS.

Het netwerk van TJIP in Delft beschikt straks over native IPv6 connectiviteit, het netwerk in Helmond wordt van IPv6 connectiviteit voorzien door middel van een IPv6 tunnel naar Delft. Om de data die door de tunnel gaat te beveiligen zal de tunnel zelf door een VPN tunnel wordt geleid.

Wanneer de nieuwe routers / firewalls zijn geconfigureerd zullen deze worden aangemerkt als Default Gateway in de DHCP servers voor de netwerken. De oude routers zullen dan worden uitgeschakeld.

Als het IPv6 netwerk actief is zullen de meeste systemen dit automatische gaan gebruiken. Dit komt omdat IPv6 door de systemen geprefereerd wordt boven IPv4.

Bij Windows XP en Server 2003 systemen waarbij IPv6 connectiviteit gewenst is dient het IPv6 protocol ingeschakeld te worden.

Hieruit volgt het volgende stappenplan

Stappenplan

Om duidelijk te maken hoe een migratie naar IPv6 eruit kan zien wordt in hieronder stap voor stap aangegeven hoe dit kan gebeuren.

1. Installeren van nieuwe MS Server 2008 R2 domain controllers in Delft en Helmond
2. Configureren van DHCPv4, DHCPv6 en DNS op de nieuwe domain controllers
3. Uitschakelen DHCP service op de huidige DHCP server in Delft en Helmond
4. Inschakelen van de DHCP services op de nieuwe domain controllers
5. Synchroniseren van DNS met de nieuwe domain controllers
6. Installeren en configureren van de nieuwe router / firewall in Delft en Helmond
7. Configureren van de IPv6 tunnel tussen Delft en Helmond
8. Aanpassen van de default gateway in de DHCP servers zodat de nieuwe routers in Delft en Helmond als default gateway worden aangemerkt.
9. Oude routers uitschakelen en de externe IPv4-adressen hiervan toevoegen op de nieuwe routers
10. Router Advertisement activeren op de nieuwe routers in Delft en Helmond
11. Eventuele Windows XP en Server 2003 systemen voorzien van het IPv6 protocol

Als de elf stappen van hierboven zijn uitgevoerd beschikt TJIP over een actieve IPv6 configuratie in Delft en Helmond waarover medewerkers het IPv6 internet zullen benaderen.

7 BRONNEN

- Charles M. Kozierok, ICMPv6 Router Advertisement and Router Solicitation Messages, http://www.tcpipguide.com/free/t_ICMPv6RouterAdvertisementandRouterSolicitationMess.htm (19 april 2011)
- Fengnet.com, http://fengnet.com/book/CCIE%20Professional%20Development%20Routing%20TCPIP%20Volume%20I/ch02lev1sec5.html (19 mei 2011)
- François Kooman, IPv6 Case Study (februari 2010)
- IPv6INT.net, http://ipv6int.net/software/index.html (3 maart 2011)
- Lakshmi, Secure-Neighbor-Discovery, http://ipv6.com/articles/research/Secure-Neighbor-Discovery.htm (14 april 2011)
- Microsoft, http://support.microsoft.com/kb/195686 (20 mei 2011)
- Paul Hoogsteder van Meanie
- Teamdhcp, Understanding of address configuration in automatic mode and installation of DHCPv6 Server, http://blogs.technet.com/b/teamdhcp/archive/2009/03/03/dhcpv6-understanding-of-address-configuration-in-automatic-mode-and-installation-of-dhcpv6-server.aspx (19 april 2011)
- Wikipedia, http://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol (9 mei 2011)
- VMWare, IPv6 Support in VMware® Infrastructure 3 (2008)