Checklist IPv6 Implementatie

Versie 3.0
Datum: 20180709

1. Inleiding

Het Internet Protocol (IP) vormt de basis van het Internet. Elke computer op het Internet heeft een nummer, een soort adres. Door deze IP-adressen weten computers elkaar te vinden en is er dus communicatie over het Internet mogelijk. Om er voor te zorgen dat iedereen hiervoor dezelfde afspraken hanteert, is in 1981 het Internet Protocol versie 4 (IPv4) ontwikkeld. Dit protocol biedt maximaal ruimte aan vier miljard adressen (en door het gebruik van (sub)netten is de werkelijke beschikbare ruimte nog kleiner).
Dat leek twintig jaar geleden misschien genoeg, maar met een toenemend aantal machines dat met het Internet verbonden wordt – pc's, mobiele telefoons, Personal Digital Assistants (PDA's), huishoudelijke apparatuur, sensoren, camera's etc. – neemt de behoefte aan nummers toe. Daarbij komt de opkomst van Internet in landen als China en India met hun miljarden inwoners. Door deze ontwikkelingen dreigt een tekort aan IP-adressen.

Vandaar dat er een nieuwe versie van het Internet Protocol werd ontwikkeld: IP versie 6. Met deze nieuwe versie komen er vele malen meer Internetadressen beschikbaar, namelijk 2^{128} of 340282366920938463463374607431768211456 om precies te zijn. Omdat er nu zo veel adressen beschikbaar zijn, kunnen organisaties ook anders omgaan met het uitdelen van IP adressen. Was het bij IPv4 nog noodzaak om geen adressen te verspillen, met IPv6 kan er gekeken worden naar een andere indeling van de adressen. Zo kunnen organisatie een indeling maken op gebied van gebouw of verdieping met IP-adressen. Over deze nummerplannen is een Handleiding Nummerplannen geschreven.

Daarnaast biedt IP versie 6 diverse verbeteringen. Zo biedt IPv6 nieuwe mogelijkheden op het gebied van geïntegreerde autoconfiguraties voor plug-and-play mogelijkheden. Apparatuur die overweg kan met IPv6 zal in staat zijn om zichzelf te configureren, waardoor het gebruik van IP eenvoudiger wordt. Verder biedt IPv6 nieuwe mogelijkheden op het gebied van beveiliging. Zo ondersteunt IPv6 standaard IPsec. Daarnaast zal het mogelijk zijn om met IPv6 data versleuteld te verzenden. Hierdoor wordt het zeer moeilijk gemaakt om zonder toestemming gevoelige data te onderscheppen en te bekijken.

Dit document bevat de checklist die u kunt gebruiken om bij uw organisatie IPv6 te implementeren

2. Fasering

In dit document wordt gewerkt met een fasering, die is afgeleid van de aanpak die VNG Realisatie en de VNG voorstellen t.a.v. de implementatie van IPv6. Zo is het de bedoeling dat op zo kort mogelijke termijn alle gemeentelijke websites en externe mailservers zo worden ingericht dat ze ook via IPv6 bereikbaar zijn (via IPv4 is dit al het geval). Ook wordt gemeenten aangeraden, dat zij zodra aan de orde, de planning voor het implementeren in de interne organisatie uitwerken. Het uitwerken van die planning is minder urgent, wanneer de bestaande interne netwerken van een gemeente nog voldoen en er geen aanleiding is om apparatuur en/of software te vervangen. De primaire doelstelling is alle Nederlandse gemeenten begin 2020 extern bereikbaar zijn via IPv6 en dat mailverkeer van en naar de gemeente via IPv6 mogelijk is. De interne uitrol van IPv6 kan op een later stadium plaatsvinden en zal per gemeenten verschillen qua realisatie. Wanneer de gemeente extern via IPv6 bereikbaar is dan zullen op enig moment ook maatregelen moeten worden getroffen om het verkeer dat via IPv6 binnen komt 'te vertalen' naar IPv4 en omgekeerd. Het moment en de wijze waarop dat gebeurt wordt door de gemeente zelf bepaald.

3. Algemeen

1. Zorg dat uw organisatie te allen tijde (extern) via het Internet bereikbaar is (website en mail).
2. De implementatie van IPv6 is niet een eenvoudige extrapolatie of omnummering van de bestaande IPv4 adresindeling. Beschouw de invoering van IPv6 van meet af aan als het toevoegen van een volledig nieuwe laag in uw netwerkinfrastructuur, naast de al bestaande IPv4 laag.
3. Neem, wanneer dat nog niet is gebeurd, IPv6 als verplichte standaard op bij alle nieuw te verwerven hardware en software en verwerk deze standaard in alle aanbestedings- en inkoopeisen (zie: https://www.ripe.net/ripe/docs/ripe-554).
4. Bepaal bij iedere nieuwe aanschaffing van hard- en software die IPv4 gebaseerd is, of die verwerving echt noodzakelijk is en/of kan worden aangehouden totdat IPv6 is geïmplementeerd. Let op met IPv6-only en IPv4 only apparatuur: die hardware kan uw toekomstige ontwikkeling beperken; de voorkeur heeft altijd dual capable apparatuur.
5. Werk altijd met een proef- of pilot opstelling voordat u met het nieuwe IPv6 adresprotocol in productie gaat.
6. Ga na welke projecten, nu en in de voorzienbare toekomst door IPv6 worden beïnvloed. Denk daarbij bijvoorbeeld aan voorgenomen vervangingen van hardware, software, effecten van aanbestedingen, collectieve inkoop van vaste verbindingen, aansluiting op de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI), (voorgenomen) samenwerking en nieuwe wet- en regelgeving, zoals AVG en Omgevingswet.

4. Voorbereidingen Fase 1 (websites en mailservers via IPv6 bereikbaar maken)

7. Formuleer een eenduidige en heldere onderbouwing voor de implementatie van IPv6. Benoem daarin de voordelen, die IPv6 heeft in vergelijking tot IPv4. Wijs daarbij op de huidige en toekomstige producten en diensten, die vaste IP adressen vragen (o.a. als gevolg van nieuwe ontwikkelingen uit DA2020 en Samen Organiseren). Argumenten in dit verband zijn:
    a. Meer unieke adressen beschikbaar
    b. Nieuwe mogelijkheden voor het indelen van adressen in relatie tot de werkwijze van de organisatie en de verdeling van werkprocessen,
    c. Betere mogelijkheden voor beveiliging, compartimentering en beheer,
    d. Let ook op de ontwikkeling rond GGI en bijv. Diginetwerk.
8. Creëer (financiële) ruimte voor o.a. het uitvoeren van scans, het opleiden van specialisten en eventueel aanpassen/vervangen van netwerkcomponenten.
9. Zoek contact met de projectorganisatie van VNG Realisatie en de implementatie/ accountmanager die voor uw regio verantwoordelijk is.
10. Zoek contact met uw belangrijke hard- en softwareleveranciers wanneer u uw IT infrastructuur en applicatielandschap geheel of gedeeltelijk extern laat beheren.
11. Activeer het voor u gereserveerde nummerblok binnen het overheidsbrede IPv6-nummerplankader door middel van het aanvraagformulier dat VNG Realisatie heeft gepubliceerd (https://www.da2020.nl/ipv6) .
12. Zoek contact met collega gemeenten in uw regio waarmee u kennis en capaciteit eventueel kunt delen. Kijk in dit verband ook naar mogelijkheden om eventueel gezamenlijk afspraken te maken met leveranciers.
13. Bepaal in hoeverre u beschikt over de noodzakelijk capaciteit en deskundigheid om gedurende een langere periode (2-3 jaar) de implementatie van IPv6 uit te voeren. Bepaal indien mogelijk ook waar, wanneer en hoe u eventueel externe capaciteit/deskundigheid gaat inzetten. In de praktijk zal doorgaans een mix ontstaan van eigen en externe capaciteit.

14. Beschouw de implementatie van IPv6 als een reguliere, zij het majeure change en pas het changeproces ook toe zoals gebruikelijk, met inbegrip van alle daarbij behorende (o.a. kwaliteitsmanagement) maatregelen.
15. Richt een projectorganisatie op die wordt ingezet om de implementatie van IPv6 op te stellen, uit te voeren en te bewaken. In deze projectorganisatie moeten zowel technisch inhoudelijke specialisten als managers en gebruikers zijn opgenomen.
16. Maak een projectplan voor de implementatie waarbij onderscheid wordt gemaakt in acties gericht op:
    a. Core/backbone van de organisatie
    b. Datacenter(s)
    c. Intern netwerk
    d. Extern netwerk/DMZ/Internet
    e. Externe verbindingen naar besloten overheidsnetwerken en naar leveranciers
17. Leg alle uitkomsten en resultaten vast, die u in deze fase heeft verzameld. Deze dienen als basis voor de verdere voorbereiding en uitwerking. Deel die resultaten ook met zowel de business- als technisch/inhoudelijk betrokkenen.
18. Maak een plan voor een proef of pilot opstelling waarin u de uitwerking van uw plan kunt toetsen. Indien u met externe leveranciers en providers werkt, doe dast dan met hen samen.

5. Uitvoering Fase 1 (websites en mailservers via IPv6 bereikbaar maken)

19. Bepaal welke websites via IPv6 bereikbaar moeten zijn. Stel per website vast wie voor de implementatie van IPv6 op die betreffende website verantwoordelijk is. Stem met deze partij af en leg de afspraken vast.
20. Bepaal welke (externe) domeinen via IPv6 bereikbaar moeten zijn. Stel per mailserver vast wie voor de implementatie van IPv6 op die betreffende server verantwoordelijk is. Stem met deze partij af en leg de afspraken vast.
21. Maak een offline proefopstelling en wanneer die uitgebreid en met succes is getest, zet het geheel dan in productie.
22. Voer de wijzigingen op de websites en de mailserver(s) door.
23. Combineer de invoering van IPv6 zo mogelijk met het invoeren van de verplichte veiligheidsstandaarden zoals TLS, DNSSEC, DMARC, DKIM, SPF, STARTTLS en DANE.
24. Voer na implementatie de compliancytest uit bijv. via Internet.nl

6. Voorbereiding Fase 2 (Invoering IPv6 in de interne organisatie)

25. Neem de Handleiding IPv6 Nummerplan eerst goed door.
26. Leid de betrokken implementatie-medewerkers op, zodat zij tijdig beschikken over alle noodzakelijke kennis en inzicht in IPv6.
27. Benut de ruimte die de adresopbouw van IPv6 u biedt: in de IPv4 adrestoewijzing is altijd rekening gehouden met het minimaliseren van adresgebruik. Vermijdt een dergelijke benadering bij de indeling van IPv6 en hou rekening met toekomstige ontwikkelingen, met een scope van minimaal 5-10 jaar. (Denk aan mogelijk voorgenomen samenwerkingen, uitbesteding van taken, effecten nieuwe wetgeving, herverdeling van taken etc.)
28. Breng in kaart wanneer netwerkcomponenten en softwareapplicaties worden vervangen. Dat is een natuurlijk moment om op IPv6 over te gaan voor het betreffende device of applicatie. Zorg ook dat de upgrade naar IPv6 wordt meegenomen in de reguliere cyclus van nieuwe releases.

29. Benader (opnieuw) uw hard- en softwareleveranciers met de vraag of de bij u geïnstalleerde hard- en software IPv6 compliant is. Ga ook na of er sprake is van zelf ontwikkelde tools waarvoor IPv6 compliancy relevant is.
30. Bepaal de implementatievolgorde zo, dat u begint bij de onderdelen die naar verwachting de minste problemen opleveren en werk vandaar uit geleidelijk naar de onderdelen die meer aandacht en impact hebben. Doe dat eerst weer in een proef- of pilotopstelling, die na goed testresultaat in productie kan gaan.
31. Zorg dat u een IPAM tool ter beschikking heeft (zie ook: https://msdn.microsoft.com/nl-nl/library/jj878331(v=ws.11).aspx).
32. Inventariseer wat en hoe het gebruik is van IPv4 bij netwerken en services. Ga daarbij na waar op dit moment al knelpunten en problemen bestaan en los die op, resp. omzeil ze zodra de implementatie van IPv6 aan de orde komt.
33. Stem af met uw beveiligingsspecialist(en). IPv6 werkt met een andere inrichting dan IPv4 als het gaat om firewalls en NAT. IPv6 leunt sterk op ICMPv6 voor de dagelijkse operaties (zie ook https://nl.wikipedia.org/wiki/Internet_Control_Message_Protocol). Iedere policy die alle ICMP packets blokt moet worden aangepast. Kijk ook in RFC 4890 hoe ICMPv6 moet worden gefilterd en wat niet mag worden geblokt.
34. Realiseer u dat IPv6 niet werkt met NAT. NAT wordt vaak ten onrechte als een beveiligingsmaatregel beschouwd, terwijl dat maar een beperkte impact heeft op de veiligheid. In plaats van NAT vereist IPv6 een stateful inspection firewall. Dit heeft duidelijke voordelen m.b.t. de veiligheid van het netwerk en moet bij IPv6 worden gebruikt in vrijwel alle gevallen waar bij IPv4 NAT werd toegepast.
35. Onderzoek of alle services en applicaties die momenteel in gebruik zijn compliant zijn voor IPv6.
36. Onderzoek of het alle (fysieke) netwerkcomponenten compliant zijn met IPv6.
37. Voer een risicoanalyse uit voor het geval IPv6 geheel of gedeeltelijk niet kan worden ingevoerd. Bepaal daarin wat de risico's zijn voor IT en voor de organisatie in het algemeen.
38. Ontwikkeling een IPv6 nummerplan (dual stack) voor de gehele organisatie, met gebruik making van de Handleiding Nummerplannen die daarvoor de Logius/VNG Realisatie is ontwikkeld.
39. Richt uw initieel nummerplan zo in dat de volledige ruimte wordt gebruikt om de gehele organisatie te bedienen. Ga daarbij uit van de Handleiding Nummerplan IPv6. Wees zeer terughoudend met het toewijzen van sequentiële subnetten, omdat die toekomstige aanpassingen sterk kunnen frustreren.
40. Simuleer de concept indeling en evalueer het initieel nummerplan met de direct betrokkenen voordat het feitelijk wordt geïmplementeerd en verwerk de resultaten van de evaluatie in een 2e versie ontwerp nummerplan, dat wordt geïmplementeerd.
41. Stel een plan op voor de implementatie van IPv6 voor de gehele interne organisatie.
42. Richt een vast coördinatiepunt in uw organisatie waar alle informatie m.b.t. de voortgang technisch en organisatorisch wordt bijgehouden.

7. Uitwerking Fase 2 (invoering IPv6 in de interne organisatie)

43. Stem met alle betrokkenen af om de volgende stap in de implementatie van IPv6 voor te bereiden. Maak daarbij een logische indeling van afdelingen/gebieden in uw organisatie die u in één doorgaande beweging voorziet van IPv6 adressen.
44. Voer het in de vorige fase ontwikkelde nummerplan in.
45. Evalueer de invoering en stel zo nodig de realisatie bij.
46. Zodra IPv6 is geïmplementeerd is er een nieuwe toegang tot uw organisatie, die consequenties heeft voor de beveiliging. Houd er rekening mee dat bepaalde systemen en applicaties van huis

uit IPv6 compliant zijn en zorg dat eventuele open entrypoints worden geblokkeerd totdat IPv6 volledig is geïmplementeerd (inclusief de bijbehorende beveiligingsmaatregelen).

47. M.b.t. legacy IPv6 only apparatuur en het t.z.t. uitfaseren van IPv4 dient een apart plan te worden ontwikkeld. Om dat te kunnen realiseren is het van belang om die apparatuur duidelijk te lokaliseren.

Meer weten?

Kijk ook op https://www.da2020.nl/ipv6

Of neem contact op met de projectgroep IPv6 van VNG Realisatie via info@vng.nl