

Van IPv4 naar IPv6

Organisaties die het Internet Protocol (IP) gebruiken voor beveiligingsdoeleinden en aanbieders van beveiligingsproducten ontkomen de komende jaren niet aan de overgang naar het nieuwe protocol IPv6. Enerzijds is het gelukkig dat die overgang niet op één dag wereldwijd zal plaatsvinden, er is geen 'IP-wereldconversiedag'. Anderzijds betekent het wel dat organisaties zelf de overgang moeten gaan voorbereiden.

Internettechnologie is gebaseerd op een stapeling van zogenaamde protocollen: TCP/IP. Deze protocollen zijn wereldwijde afspraken waarmee de communicatie tussen verschillende apparaten en computers is geregeld. Sinds de jaren tachtig is versie 4 van het internetprotocol (IP) wereldwijd in gebruik. IP verzorgt de pakketgewijze gegevenstransporten over verschillende transportmedia als glasvezel, kabel en de ether. Om de pakketten correct van

de zender naar de ontvanger te krijgen, gebruikt IP een adresseringssysteem. Bij de opzet zo'n twintig jaar geleden van IP versie 4 (IPv4) is uitgegaan dat de vier miljard mogelijke computeradressen ruim voldoende zouden zijn. Geen rekening was gehouden met de explosie aan communicatie die internet teweeg heeft gebracht, de opkomst van elektronische agenda's, mobieltjes, de vele websites en de grote groepen nieuwe internetgebruikers (bijvoorbeeld Chinezen en Indiërs).

Midden in de jaren negentig werd voorzien dat het aantal internetadressen snel aan het opraken was. Daarop zijn een aantal organisatorische en technische maatregelen getroffen om dat probleem naar achteren te schuiven. Zo kon een organisatie geen grote hoeveelheden IP-adressen meer verkrijgen en werd de Network Address Translation technologie (NAT) geïntroduceerd waardoor de vele systemen op interne netwerken niet allemaal een officieel internetadres nodig hadden. Tegelijkertijd werd eind jaren negentig een aantal tekortkomingen van IPv4 op het gebied van beveiliging duidelijk. Hierbij kan worden gedacht aan de denial-of-service aanvallen op netwerken. De Internet Engineering Task Force (IETF) heeft daarop het IP Next Generation (IPng) project gestart waarbij verschillende opties werden onderzocht om de gerezen IPv4 problemen aan te pakken. Uiteindelijk heeft dat geresulteerd in de vaststelling van het IP versie 6 (IPv6) protocol (*1) en een aantal verwante

protocollen die onder andere mobiel internetten mogelijk maken. Na een lange testperiode van IPng door universiteiten en software- en hardwareontwikkelaars en enkele technische aanpassingen van de de facto standaard, wordt IPv6 al enkele jaren operationeel gebruikt door een aantal pioniers en worden sinds 2002 IPv6 diensten door ISPs in Nederland aangeboden. Overigens gebruiken de moderne UMTS mobieltjes ook IPv6.

Uniek Met de uitgebreide adresseringsruimte van 2 tot de macht 128 zijn 340.282.366.920.938.463.463.374.607.431.768.211.456 adressen mogelijk. Dat is ruim voldoende om ieder mobieltje, camera, deurbel, koelkast, stopcontact, airbag, gladheidsensor, remtrommel, autoband, koelkast en wat we in de komende jaren nog meer op de aarde elektronisch willen benaderen uniek te adresseren. Om de te verwachten explosie aan communicerende apparaten en sensoren eenvoudiger, maar ook veiliger aan netwerken te kunnen laten deelnemen, ondersteunt IPv6 ook nieuwe diensten. Bijvoorbeeld autoconfiguratie ('plug-and-play'), IPSec (veiligheidsopaties voor exclusiviteit en integriteit) en een betere ondersteuning voor mobiel internetten zoals 'roaming' - het transparant gebruik van andere netwerken en het automatisch overstappen naar een ander netwerk - niet alleen van een enkel apparaat, maar van hele netwerken tegelijk. Andere, meer technische aanpassingen, betreffen ondersteuning

Management-summary

De huidige internettechnologie, gebaseerd op het Internet Protocol versie 4 (IPv4), loopt tegen een aantal beperkingen aan zoals het wereldwijd opraken van het aantal vrije internetadressen. Nieuwe technologie gebaseerd op het IPv6 protocol moet de problemen oplossen. Dat heeft ook consequenties voor organisaties die in toenemende mate gebruik maken van op IP-gebaseerde beveiligingsproducten. De overgang naar IPv6 wordt niet opgelegd zoals eertijds de wijziging van de netnummerindeling in Nederland naar een tiencijferig systeem, maar is de verantwoordelijkheid van iedere organisatie zelf. Verwacht wordt dat organisaties ergens tussen nu en 2015 zullen moeten migreren naar IPv6.

*1) IP versie 5 is een heel specifieke versie van IP die ontworpen is voor heel specifieke real-time defensietoepassingen zoals de koppeling van systemen voor pilotentrainingen.



van quality-of-service, prioriteitsverkeer en betere multicasting voor bijvoorbeeld web-TV toepassingen.

Overgang Organisaties kunnen vandaag starten met IP versie 6 mits zij gebruik maken van apparatuur die 'IPv6 ready' is en zij deze mogelijkheid activeren op hun Linux, UNIX, Windows XP, VISTA of Windows Server systeem. Naast het draaien van IPv6 op alle systemen die moeten communiceren, dienen er ook een aantal diensten in het netwerk te worden geïnstalleerd. Dit vergt enige studie door de netwerkbeheerders. Overigens leveren een aantal ISPs en mobiele operators, zoals SURFnet, XS4ALL en T-Mobile, al een

IPv6 noch wereldwijd, noch in de meeste organisaties op één moment kan plaatsvinden. Mits goed geïmplementeerd en indien aan enkele adresrestricties wordt voldaan, kunnen beide protocollen naast elkaar op eenzelfde fysiek netwerk leven. Ook is het mogelijk om alle IPv4 verkeer in te pakken in een IPv6 pakketstroom en deze transparant over een IPv6 netwerk naar een andere locatie te leiden via een zogenaamde tunnel. Dat is wellicht een handige optie tijdens de migratie van het netwerk. Het omgekeerde, een IPv6 tunnel in een IPv4 netwerk, is ook mogelijk. Dat kan handig zijn voor IPv6 experimenten die meer locaties in een organisatie omvatten. Daarnaast zijn er

systemen die al onder IPv6 draaien.

Wanneer migreren? Tenzij een organisatie een voorloper wil zijn in het omzetten van beveiligingstoepassingen op IPv6 of indien een ICT-organisatie snel wil migreren, is dit op heel korte termijn veelal nog niet aan de orde. Technisch gezien zijn er voor veel organisaties weinig redenen om nu een IPv4 naar IPv6 migratie in te zetten. Veel IPv6-apparatuur en programmatuur is nog niet lang op de markt en kan nog enige kinderziekten vertonen. Verder is een behoorlijke leercurve nodig voor de netwerkbeheerders. Zij moeten ervaring krijgen met IPv6 zoals het juist en veilig configureren, en het tijdig elimineren

IPv6: bent u er tijdig klaar voor of wordt u onaangenaam verrast?

aantal jaren IPv6 connecties over ADSL, de kabel en mobiel. Het is dus mogelijk thuis met IPv6 te experimenteren! Bij het ontwerp van IPv6 was het duidelijk dat de overgang van IPv4 naar

systemen in het netwerk te plaatsen met twee 'stacks': één die IPv4 'praat' en één die IPv6 'praat'. Deze systemen kunnen als vertaler werken tussen systemen die nog IPv4 gebruiken en de

van storingen en problemen. Als een organisatie zich de komende jaren echter niet tijdig verdiept in een overgang, kan deze door apparatuurgebrek of door gebrek aan IPv4-adressen voor

externe aansluitingen ineens worden gedwongen tot een veel snellere overgang dan gewenst.

Een reden om wel snel te migreren is dat de kosten voor het verkrijgen van een extra IP-adres wellicht snel gaan oplopen daar de IPv4-adressen naar schatting van sommige bronnen rond 2013 en volgens het 'IPv4 Address Report' zelfs rond december 2010 definitief opraken. Verder zal IPv6 de komende tijd de standaard worden waarmee nieuwe apparatuur uitgeleverd gaat worden; IPv4 installeren zal extra inspanning gaan vergen. Ook beloven de autoconfiguratiemechanismen in IPv6 een daling van de beheerskosten, zeker als het een groot netwerk betreft met vele componenten, beveiligings- en bewakingssensoren, camera's en dergelijke.

Aanpak Niemand ontkomt op termijn niet aan een overgang. Tijdig voorbereiden is aan te bevelen boven ineens te worden geconfronteerd met de noodzaak om op (te) korte termijn te migreren. Een aanpak op hoofdlijnen bevat de volgende stappen:

1. Verdiep u in de toekomstverwachtingen van uw netwerk, het aantal computers, beveiligingssensoren, camera's en

andere systemen. Denkt u andere locaties op afstand te koppelen? Hoeveel openbare IP-adressen heeft u nodig? Zijn die op termijn beschikbaar? Wat is de business case? Stel daarmee een lange termijn IPv4 - IPv6 transitieplan op.

2. Schaf vanaf heden alleen computersystemen, apparatuur, sensoren en IP-camera's aan die IPv6-gereed zijn. Niet tijdig investeren in IPv6 apparatuur betekent op het moment dat u gedwongen over moet, u wellicht een grote afschrijvingspost heeft en tegelijk veel extra investeringen heeft.
3. Laat uw netwerkbeheerders in de komende jaren kennis opdoen van IPv6 door het volgen van cursussen, het lezen van boeken en ervaringen op het internet en vooral het gericht experimenteren met apparatuur die u standaard gebruikt (de speciale systemen zijn met enig verlies aan snelheid achter een 'dual stack' te plaatsen).
4. Zet een adresseringsplan op en start een pilot invoeringsproject.
5. Converteer in een aantal stappen waarbij u gebruik maakt van de ervaringen van organisaties die uw organisatie voorgingen. Door Economische Zaken is, als uitvloeisel van een EU-actie, in Nederland een IPv6 Task Force gestart die een snelle conversie naar IPv6 wil bevorderen en de komende tijd meer informatie beschikbaar zal stellen.

Tot slot, BEVEILIGING zal ook een vinger aan de pols houden en regelmatig over de IPv6-ontwikkelingen en beveiligingsapparatuur en -sensoren gaan rapporteren.

MEER INFORMATIE

www.ipv6-taskforce.nl: website van de IP versie 6 Task Force met links naar websites met artikelen over IPv6 en ervaringen van anderen.

www.ipv6tf.org: website van de Europese IPv6 transitie.

Onderzoek naar praktische implementaties van Internet Protocol versie 6, een publicatie geschreven voor ECP.NL/Economische Zaken door Peter van Eijk.

www.ecp.nl/download/Rapport_IPv6_7_maart_2007_definitief.pdf

■ **Ir. Eric Luijff**
Eric.Luijff@beveiliging.nl