SURFnet-rapport

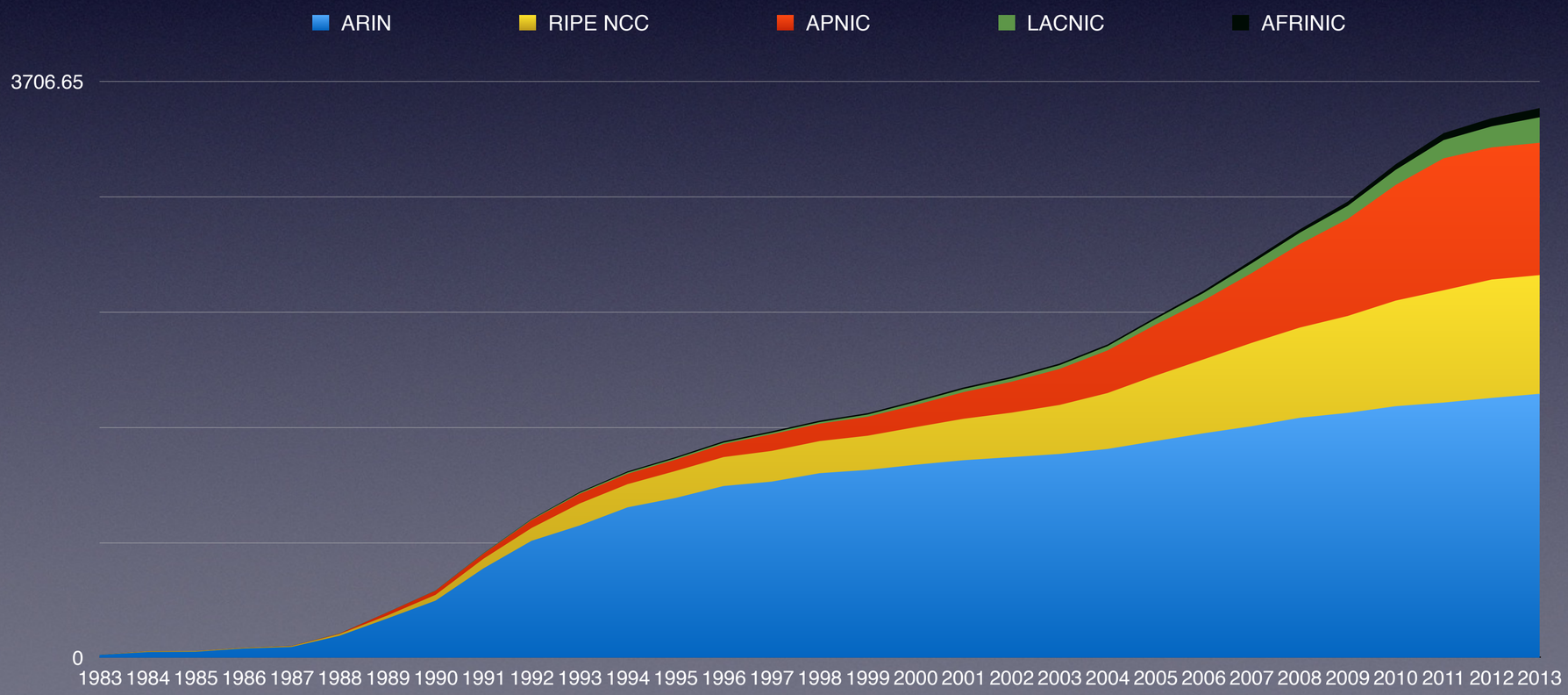
IPv6 beveiliging

Utrecht, 17 juni 2014

Iljitsch van Beijnum

Terzijde: IPv4 is op!

- With the Americas running out of IPv4, it's official: The Internet is full (Ars Technica)
- Waar zijn de IPv4-adressen gebleven? (ISP Today)



Het rapport

- In opdracht van SURFnet
- Doelgroep: beheerders van campusnetwerken
- Geschreven door mij 😀
  - de niet-gelover in firewalls! 😬
- In het Engels en het Nederlands

2. Kenmerken IPv6

- Adresnotatie, adresconfiguratie, geen NAT
- Gebruikers identificeren adhv IPv6-adres
  - omgekeerde probleem als bij IPv4: in plaats van meerdere gebruikers/adres, meerdere adressen/ gebruiker!
  - (bijna) geen waterdichte oplossing
- IPsec niet meer "verplicht" met RFC 4294 → 6434

2. Kenmerken IPv6 (2)

- Pas op met link-locals
  - zelfs als je geen IPv6 aan hebt staan!
- SEND: SEcure Neighbor Discovery
  - veilig!
  - alleen nauwelijks/geen implementaties...
- Hop Limit = 255 voor lokale pakketten

3. Migratie/coexistentie

- Grootste probleem: 6to4 staat aan uit de doos onder Windows, als ook internet connection sharing aanstaat worden er router advertisements gestuurd en kunnen kan het IPv6-verkeer van *andere* systemen via de tunnel gaan

4. IPv6-risico's

- Scannen!
- In kaart brengen via multicast
- ND cache exhaustion (uitputting?)
- Ongeautoriseerde RAs (RA Guard)
- Ongeautoriseerde DHCPv6 servers?
  - afhankelijk van M en O bits in RA
  - risico injectie kwaadaardige DNS-adressen

Ongeautoriseerde DHCPv6 servers

Tabel 1, M en O bits in Router Advertisements en gebruik van DHCPv6

Soort network	M en O bits	Impact ongeautoriseerde DHCPv6-server
DHCPv6 wordt gebruikt voor adresconfigurattie	M = 1	Aanvaller kan adresconfiguratie ontregelen en adressen kwaadaardige DNS-servers injecteren
DHCPv6 wordt gebruikt voor overige congfiguratie (DNS etc.)	M = 0, O = 1	Aanvaller kan adressen kwaadaardige DNS-servers injecteren
DHCPv6 wordt niet gebruikt	M = 0, O = 0	Geen impact, hosts maken geen contact met DHCPv6-server

5. Adresseren risico's

- Afweging: gebruikersgemak vs veiligheid
  - verschilt per subnet!
- Filteren extra (extension) headers en fragmentatie
- Soorten firewalls:
  - hardware IPv4-firewall: laat geen IPv6 door
  - software IPv4-firewall: laat alle IPv6 door

SEND, statische ND/MAC

Tabel 2, adresconfiguratiewijzen met en zonder SEND en statische ND/MAC-tabellen

	Op zichzelf	Met SEND	Met statische ND/MAC-tabellen
Handmatige configuratie	Geen autoconfig, kapen IP/MAC en DoS mogelijk	Geen autoconfig, kapen IP onmogelijk, MAC DoS wel	Geen autoconfig, kapen IP/MAC en DoS onmogelijk
Stateless autoconfig	Moeilijk om IP-adressen te loggen, kapen IP/MAC en DoS mogelijk	Loggen makkelijker, kapen IP onmogelijk, MAC DoS wel	Statisch ND onmogelijk, statisch MAC maakt loggen makkelijker, DoS moeilijker
DHCPv6	Makkelijk om IP-adressen te loggen, kapen IP/MAC en DoS mogelijk	Makkelijk om IP-adressen te loggen, kapen IP onmogelijk, MAC DoS wel	Per-host DHCP-config vereist, kapen IP/MAC en DoS onmogelijk

5. Adresseren risico's (2)

- Stateful firewall in plaats van NAT
- Filteren ICMPv6 en sommige adresreeksen
  - default permit vs default deny
    - (brand ik mijn vingers niet aan...)
  - belangrijk: hetzelfde voor IPv4 en IPv6!
- Filteren op prefixlengte in BGP

Tabel 3, filterimplicaties van IPv6-prefixen

Prefix	Eerste bits	Doel	Filterimplicaties
::/3	000	Speciale doeleinden	Kan gefilterd worden aan rand netwerk
::1/128		Localhost	In hosts: niet filteren / wees voorzichtig*
::ffff:0:0/96		IPv4-mapped API adressen	In hosts: niet filteren / wees voorzichtig*
64:ff9b::/96	0000 0000 0110 0100	NAT64 well-known prefix	Filter aan rand netwerk
2000::/3	001	Global unicast	Niet filteren
2001::/32		Teredo	Filteren kan in enkel geval tot timeouts leiden
2002::/16	0010 0000 0000 0010	6to4	Filteren leidt soms tot timeouts
4000::/2 - f800::/6	01 - 1111 01	Gereserveerd	Filter alleen als er een updateprocedure is
fc00::/7	1111 110	Unique Site Local	Filter aan rand netwerk
fe80::/10	1111 1110 01	Link-local	Niet filteren / wees voorzich-tig**, gaat niet door routers
fec0::/10	1111 1110 11	Oude site-local	Filter
ff00::/8	1111 1111	Multicast	Filter niet, maar doe alleen multicastrouting waar nodig

Tabel 4, filterimplicaties van ICMPv6-foutmeldingen

Type	Naam	Doel	Filterimplicaties
1	Destination Unreachable	Communiceert onbereik-bare bestemmingen	Filteren leidt tot timeouts
2	Packet Too Big	Path MTU Discovery	Filteren maakt communicatie met bepaalde bestemmingen onmogelijk
3	Time Exceeded	Traceroute	Filteren blokkeert traceroute, RFC 4890 beveelt doorlaten Code 0 aan
4	Parameter problem	Communiceert protocolfouten	Moeilijk te zeggen, is ongebruikelijk, RFC 4890 beveelt doorlaten Code 1 + 2 aan

Tabel 5, filterimplicaties van ICMPv6-informatieberichten

Type	Naam	Doel	Filterimplicaties
128	Echo Request	Ping	Ping werkt niet, misschien impact Teredo
129	Echo Reply	Ping	Ping werkt niet, misschien impact Teredo
130 - 132, 143	MLD	Vertelt routers waar multicasts te sturen	Multicast-applicaties zullen waarschijnlijk niet werken
133	Router Solicitation	Triggert Router Advertisement	Default gateway and adresconfiguratie zijn veel langzamer
134	Router Advertisement	Default gateway, adres-configuratie	Hosts krijgen geen default gateway en geen global unicast-adressen
135	Neighbor Solicitation	Lokale communicatie, adresconfiguratie	Hosts kunnen niet communiceren over IPv6
136	Neighbor Advertisement	Lokale communicatie, adresconfiguratie	Hosts kunnen niet communiceren over IPv6
137	Redirect Message	Optimaliseert hoe pakketten lopen	Pakketten moeten misschien langs een extra router

135	Neighbor Solicitation	Lokale communicatie, adresconfiguratie	Hosts kunnen niet communiceren over IPv6
136	Neighbor Advertisement	Lokale communicatie, adresconfiguratie	Hosts kunnen niet communiceren over IPv6
137	Redirect Message	Optimaliseert hoe pakketten lopen	Pakketten moeten misschien langs een extra router
139	Node Information Query	Debugging	Geen
140	Node Information Response	Debugging	Geen
144 - 147	Mobile IPv6	Mobile IPv6	MIPv6 werkt niet (MIPv6 is niet algemeen geïmplementeerd)
148 - 149	SEND	SEcure Neighbor Discovery	SEND werkt niet (SEND is niet algemeen geïmplementeerd)
152 - 153	Multicast Router Discovery	Optimaliseert multicast forwarding door switches (vgl. IGMP snooping)	Switches kunnen multicasts blokkeren of onnodig doorsturen

6. IPv6 uitschakelen

- Ook als je geen IPv6 aanzet in je netwerk:
  - link-locals
  - tunnels: 6to4/Teredo/...
- Filteren protocol 41, UDP poort 3544: timeouts, niet 100% effectief
- Uitschakelen per host: veel administratie!
- Filteren ethertype 0x86dd: effectief, behalve tunnels

That's all, folks!

Vragen?