Computerworld, 3. 6. 2011

Bezpečnost protokolu IPv6

V minulém dílu seriálu jsme rozebírali, jaké existují přechodové mechanismy pro zavádění protokolu IPv6. Jako nejsprávnější (leč bohužel zatím nejméně dostupnou) variantu jsme označili tzv. dual-stack, tedy zavedení protokolu IPv6 vedle protokolu IPv4. U ostatních variant, založených na nějaké formě tunelu, jsme zmínili jejich technické nevýhody a s tím spojenou sníženou kvalitu služby. Kromě zmíněných problémů, ale existují i další problematická místa tunelování. Asi nejvýraznější jsou bezpečnostní problémy, které se týkají především automatický sestavovaných tunelů.

Bezpečnost především

Ačkoliv protokol IPv6 ještě není zdaleka tak rozšířen, jak se původně předpokládalo, rozhodně jde o plnohodnotný protokol, přes který lze provozovat v podstatě stejnou škálu služeb jako přes IPv4. A to samozřejmě včetně aktivit ne zrovna vítaných, jako třeba útočení. Proto je nutné při zavádění (a dokonce ještě před zaváděním) IPv6 myslet na bezpečnost úplně stejně jako u IPv4 navíc s tím rozdílem, že v protokolu IPv6 neexistuje NAT a každá koncová stanice tak má globálně dostupnou IP adresu. Pokud je protokol IPv6 zaváděn (ať již pomocí dual-stack či tunely) informovaným správcem sítě, pravděpodobně nastaví i příslušný hraniční firewall a ochrání stanice uvnitř sítě. Problémem tunelů ale je, že je nemusí sestavovat pouze informovaný správce, ale že je může nastavit v podstatě libovolný uživatel. Takový uživatel pak obejde bezpečnostní politiku příslušné sítě a jeho koncová stanice je zcela vystavena všem uživatelům veřejného IPv6 Internetu. Nicméně to je pořád alespoň trochu v pořádku, pokud jde o vědomou akci.

Automatické tunely aneb IPv6 už tu je!

Ještě horší je, pokud operační systém sestaví IPv6 tunel zcela automaticky bez vědomí uživatele. A to se bohužel právě děje v případě operačních systémů Windows, které automaticky sestavují Teredo tunel. Bohužel díky tomu, že Teredo využívá jako transportní protokol UDP, má správce sítě poměrně omezené možnosti, jak s tímto problémem pracovat a tento fakt může mít poměrně zásadní dopad na bezpečnost celé sítě. Jak je tedy vidět, s protokolem IPv6 je nutno počítat ještě dříve, než bude fakticky zaveden.

Opačný přechodový mechanismus

Abychom zcela uzavřeli náš výčet přechodových mechanismů, musíme se ještě zmínit o opačném směru,

tedy o situaci, kdy koncová stanice s pouze IPv6 konektivitou chce přistupovat do IPv4 Internetu. Zatím se může jevit tato situace jako nesmyslná, vždyť IPv4 konektivita je přeci dostupná všude a naopak jen těžko byste dnes hledali síť, jejíž veškeré komponenty jsou plně připraveny na IPv6. Ale uvědomme si, že IPv4 adresy nám docházejí a postupem času se tato situace může stát realitou. Navíc by takováto konfigurace mohla minimalizovat náklady spojené s provozem duální logické infrastruktury v případě dual-stacku.

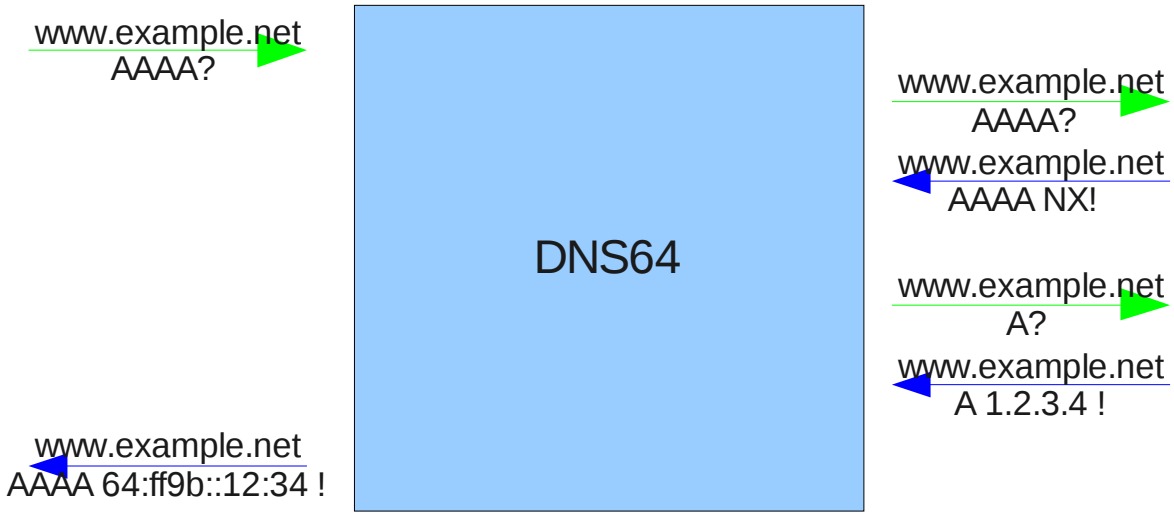
NAT64

Mechanismus, který zmiňovanou situaci řeší, se jmenuje NAT64 a byl vydán v dubnu letošního roku. Pokud se někomu jeví divné, že takovýto mechanismus byl standardizován až takto pozdě, je třeba uvést, že jde již o druhý pokus o řešení dané situace. Původní mechanismus, který se jmenoval NAT-PT, byl vydán již v únoru 2000 a byl od začátku pojat poměrně široce. Umožňoval totiž mimo jiné navázání spojení jak se strany IPv6 světa tak i ze strany opačné. Bohužel s tímto se ale vázalo mnoho provozních problémů a tak byl nakonec tento mechanismus odmítnut.

NAT64 tedy částečně navazuje na věci, které se ukázaly v NAT-PT jako smysluplné a funkční. Základní princip fungování je podobný jako u běžného NATu, který známe již z prostředí IPv4. Podobně jako u IPv4 NAT, i u NAT64 musí být branou do (IPv4) Internetu směrovač, který má jednu nebo více veřejných IPv4 adres. NAT64 je popsán v dokumentech RFC6144 až RFC6147 a je bytostně spojen s druhým mechanismem, který se nazývá DNS64.

Změny v DNS – DNS64

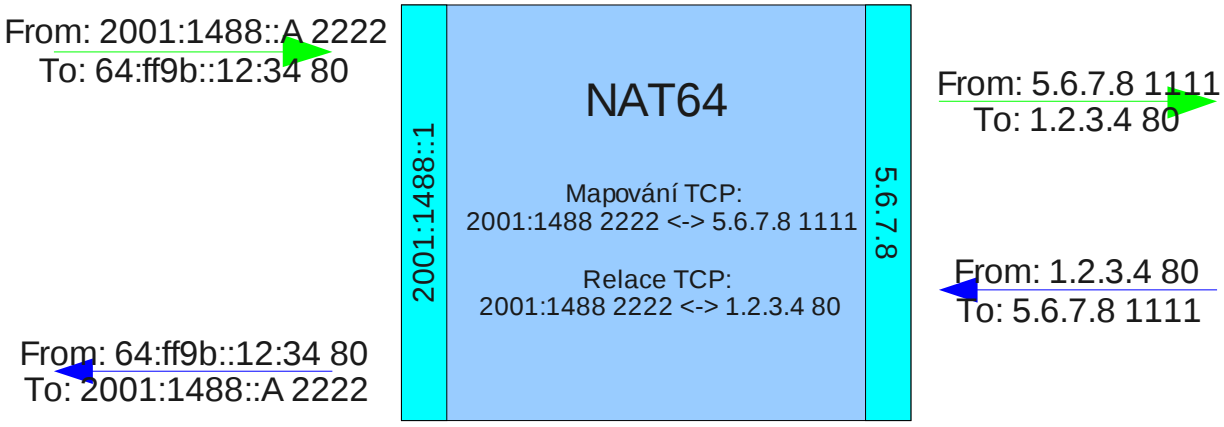
Pokud chce klient zahájit nějakou komunikaci, pokusí se vyhledat adresu pro nějaký DNS záznam. Vzhledem k tomu, že v tomto případě jde o klienta s pouze IPv6 konektivitou, pak logicky hledá AAAA nebo-li IPv6 adresu cílové služby. Tento dotaz je přeposlán na NAT64 směrovač a ten jej obyčejně přepošle do Internetu. Pokud je koncová služba dostupná pouze po IPv4 pak tento dotaz logicky selže. Nicméně v této fázi ještě směrovač klienta neinformuje, ale ještě pošle obdobný dotaz s tím rozdílem, že se ptá na A nebo-li IPv4 záznam. Odpovědí je mu IPv4 adresa cílové služby. Tu pak namapuje do IPv6 adresy. Směrovač má pro tento účel vyhrazený IPv6 prefix a IPv4 adresu do něj prostě vloží. Dejme tomu, že IPv4 služby je 1.2.3.4 a vyhrazený prefix je 64:ff9b::/96, což je mimochodem doporučovaný prefix v RFC6502. Složena adresa by tedy vypadala jako 64:ff9b::1.2.3.4 nebo-li 64:ff9b::102:304. V tomto smyslu směrovač upraví odpověď na původní dotaz a vrátí ji klientovi. Celý proces ilustruje následující obrázek.



A pak NAT

Klient tedy nyní předpokládá, že služba je dostupná pomocí protokolu IPv6 a pokusí se tedy otevřít spojení. Komunikace je od klienta opět přeposlána na směrovač, který již dle adresy pozná, že je určena pro IPv4 Internet. Aby mohl paket od klienta přeposlat, musí pro danou zdrojovou IPv6 adresu a port přidělit nějakou svou veřejnou IPv4 adresu a port. Toto své přidělení si uloží do mapovací tabulky, aby věděl, kam přeposlat odpověď, až se vrátí od serveru služby. Zároveň si ovšem musí pamatovat, že mezi čtveřicí zdrojová IPv6 adresa, port a cílová IPv4 adresa, port je aktivní spojení. Tyto záznamy si ukládá do tabulky spojení a její položky obnovuje s každým prošlým paketem. Pokud nebyla položka dlouho obnovována, je z tabulky spojení vyřazena a zároveň pokud pro položku v mapovací tabulce neexistuje žádný záznam v tabulce spojení, je vyřazena taktéž a odpovídající dvojice IPv4 adresa a port může být použita pro jiné spojení. Do mapovací tabulky se záznamy nemusí dostávat pouze dynamicky, existuje i možnost dopsat tam záznam staticky pro opačný směr, tedy případ, že by bylo vhodné poskytnout nějakou službu z IPv6 Internetu IPv4 klientům. Mapovací tabulky pochopitelně existují odděleně pro TCP a UDP (v mírně jiné formě i ICMP)

protokoly. Celý průběh mapování opět znázorňuje následující obrázek.



Problém s DNSSEC

Celý mechanismus vypadá poměrně jednoduše. Lze v něm nalézt jeden sporný bod, který se týká jeho manipulace s DNS protokolem. Díky tomu není možné jednoduše použít bezpečnostní technologii DNSSEC. Pokud by koncový klient prováděl DNSSEC validaci odpovědí, musel by ty modifikované pochopitelně zahodit, jako podvržené. Tento nedostatek lze například odstranit tím, že validaci bude pro klienty provádět právě NAT64 směrovač, který dostává DNS odpovědi ještě nemodifikované.

Tímto končí výčet přechodových mechanismů a zároveň tím končí i více teoretická část našeho seriálu. V příštím díle se pokusíme na IPv6 podívat poněkud více prakticky.

Autor:
Ondřej Filip, výkonný ředitel sdružení CZ.NIC, správce české národní domény .CZ