

Ali lahko “skriti” IPv6 promet škoduje vašemu lokalnemu omrežju?

Jan Žorž, go6.si
2. Slo IPv6 summit, 13.okt.2009



Osnove

- 6to4 tuneli delujejo tudi za IPv4 NAT-om
- Tere do promet gre čez NAT
- Tunnelbrokerji so za učenje in prve izkušnje z IPv6, ne za produkcijo.
- IPv6 požarni zid na koncu tunela?
- Kaj se nam lahko zgodi, če nimamo urejene primerne varnostne politike na našem IPv4 požarnem zidu?
- IPv4 ni več edini protokol, katerega moramo analizirati in zanj imeti varnostno politiko.

Tunel doma...

- Vzamemo prenosnika in testno postavimo 6to4 tunel na tunnelbroker
- Tunnelbroker nam dodeli /64 za tunel in /64 za lokalno mrežo
- V default navodilih je nekaj ukazov, med drugimi tudi packet forwarding ukaz
- Omogočimo router advertisement daemon in vse naprave z IPv6 stackom dobijo naslov in lahko komunicirajo.
- Dobro opravljeno, poskus uspel.

Tunel v podjetju...

- Prenosnika odnesemo naslednji dan v službo in ga priključimo na lokalno omrežje.
- Vse naprave v omrežju dobijo IPv6 naslove
- Na tunnelbrokerju spremenimo tunnel endpoint
- Tunel na tunnelbrokerja deluje...
- Packet forwarding je tudi še omogočen
- Celotno omrežje je dosegljivo iz IPv6 interneta, saj korporacijski požarni zid ne zna delati z IPv6 prometom in ga sploh ne zaznava.
- Varnostni problem?
- Odtekanje oziroma dostop do zaupnih informacij?

Ignoranca.

- IPv4 ni več edini protokol, katerega moramo poznati in obravnavati.
- IPv4 varnostna politika tudi ni več dovolj.
- IPv6 je tukaj, treba ga bo spoznati in obvladati.
- IPv6 ukinja NAT. Get over with it.
- Obstajajo IPv6 požarni zidovi
- Obstajajo IPv6 IDS/IPS/Antivirus/Antithreat naprave
- Obstajata znanje in izkušnje na tem področju

Note to everybody:

Stop moving powerpoints, start moving packets.

- Randy Bush.