IPv6 - implementazione a Ferrara

A. Gianoli, M. Gambetti - INFN Ferrara

Situazione di Ferrara

- 2 reti /24, circa 360 macchine con indirizzi “veri” (sezione + dipartimento)

- portatili su reti private con NAT (web portal, dot1x, eduroam, cavo)

- uso di VLAN per separare traffico: “normale”, “portatili” (4 diverse), stampanti, voip, management

- telefoni voip su rete università

IPv6

- 2001:760:4206::/48
- decisione di usare /64 diversa per i portatili

  2001:760:4206:0000::/64 (fissi)

  2001:760:4206:0002::/64 (portatili)

Decisione obbligata: “devi” usare /64
(e abbiamo dovuto scoprirlo…)

Cosa è stato messo sotto IPv6?

- solo dual stack
- più o meno tutto:
  - dns
  - dhcp
  - ldap
  - web
  - posta
- unico argomento che richiederà lavori: gestione portatili

Problemi: #1

- regole di firewall/ACL: manca impostazione comune
- regole “strict” (e chi le tiene aggiornate) o loose?

- …e aspettatevi problemi con youtube o con i siti che inglobano filmati da youtube

deny 3ffe::/16 le 128
deny 2001:db8::/32 le 128
permit 2001::/32
deny 2001::/32 le 128
permit 2002::/32
deny 2002::/32 le 128
deny 0000::/8 le 128
deny fe00::/9 le 128
deny ff00::/8 le 128
permit 2000::/3 le 48
deny 0::/0 le 128

E’ sufficiente?

Problemi: #2

- versioni “vecchie” di linux supportano ipv6 ma potrebbero avere i file di configurazione dei servizi non aggiornati per ipv6
- es. ntpd…

RedHat 5.8

ntp.conf

restrict -4 default nomodify nopeer noquery notrap

restrict 127.0.0.1

RedHat 6.5

ntp.conf

restrict default kod nomodify notrap nopeer noquery

restrict -6 default kod nomodify notrap nopeer noquery

restrict 127.0.0.1

restrict -6 ::1

Problemi: #3

- aka: quando il problema non siete voi… ma ne pagate le conseguenze
- nel nostro caso ha colpito la posta elettronica
- postfix default
  - prima prova ipv6 e poi prova ipv4
  - se ipv6 fallisce (trova host/porta ma non riesce a mandare) non prova ipv4
  - problemi sia a mandare che a ricevere, legati principalmente a rdns
  - anche con siti “grossi” (nasa…)

➧ disservizio per gli utenti

Cosa manca

- studio adeguato su filtro router/iptables specifico per IPv6

- abbiamo deciso di fare delle /64, ma non abbiamo studiato l'argomento

- con IPv6 i portatili, fino ad ora dietro NAT, diventano visibili: non abbiamo ragionato su pro e contro

Conclusioni

- grazie al lavoro di Gambetti potremmo avere tutto su ipv6
- dobbiamo studiare la questione “firewall”
- abbiamo rimesso email solo su ipv4 causa i vari disservizi incontrati