Sicurezza di BGP

Marco d'Itri
<md@linux.it>
@rfc1036

End Summer Camp 2K15 - Sep 5, 2015

Internet: reti indipendenti che si scambiano traffico

Internet è un insieme di **reti indipendenti interconnesse** tra di loro, quindi occorre stabilire meccanismi tecnici e accordi commerciali che permettano a tutti di raggiungere chiunque altro.

Come fa una rete a sapere come raggiungerne un'altra?

- Non esiste un coordinamento centralizzato.
- Possono esserci più percorsi, che potrebbero essere rotti in un certo momento: occorre un meccanismo dinamico.
- Ciascun lato di una interconnessione comunica all'altro per quali destinazioni vuole accettare traffico.

Internet: reti indipendenti che si scambiano traffico (2)

Gli accordi economici:

- **Cliente**: mi paga perché gli permetta di raggiungere il resto di Internet.
- **Peering**: ci accordiamo per scambiarci direttamente il traffico dei rispettivi clienti.
- **Transito**: sono io il cliente, e pago qualcuno perché mi permetta di raggiungere il resto di Internet.

Le basi del routing interdomain

Route

Le informazioni che individuano una rete, per esempio `192.175.48.0/24`, e come raggiungerla.

Il protocollo di routing BGP

- Serve per scambiare informazioni di routing dentro un autonomous system (internal BGP) o tra AS diversi (external BGP).
- Per esempio tra due peer o tra fornitore di transito e cliente

Autonomous system

- *Una entità con una unica politica di routing verso l'esterno.*
- Identificato da un numero a 32 bit. Per esempio GARR è AS137.
- Annuncia ai propri vicini le route per cui vuole ricevere traffico.

Un esempio pratico

```
md@spock> show route table inet.0 protocol bgp 192.175.48.0/24 terse

inet.0: 552304 destinations, 1425122 routes↩
  (551557 active, 12 holddown, 1188 hidden)
+ = Active Route, - = Last Active, * = Both

A V Destination      Metric 1   Metric 2  Next hop         AS path
* ? 192.175.48.0/24       150      10000                   112 I
  unverified                               >85.94.206.221
  ?                        150      10000                   12041 112 I
  unverified                               >217.29.66.124
  ?                        150      10000                   12779 112 I
  unverified                               >217.29.66.65
  ?                        150      10000                   12779 112 I
  unverified                               >217.29.66.65
  ?                        150      10000                   12779 112 I
  unverified                               >217.29.66.65
  ?                        150      10000                   6939 16668 112 I
  unverified                               >217.29.66.125
  ?                        110     100000                   2914 16876 112 E
  unverified                               >81.25.202.193
```

Sicurezza del routing

Si può inviare ai propri vicini qualsiasi route: sono loro a dovere decidere quali accettare.

Per filtrare le route ricevute si creano, più o meno automaticamente, degli elenchi di route e/o di AS con cui le confronta il router.

A volte è oggettivamente difficile filtrare i propri peer, ma occorre impegnarsi di più per migliorare la sicurezza del routing di Internet.

È ingiustificabile non filtrare i propri clienti.

Come sapere quali route qualcuno può annunciare?

Per esempio, un cliente o peer può usare:

- Record `route` o `route6` negli Internet Routing Registry (IRR), ma sono affidabili solo da RIPE e AFNIC e comunque non sempre sono tenuti aggiornati.
- Letter of authorization (LOA): può essere falsificata, richiede operazioni manuali, in pratica è usabile solo per i propri clienti.
- Attestazione crittografica mediante RPKI (origine) e BGPSEC (percorso): complesso, poco diffuso, vulnerabile ad attacchi giudiziari, aumenta la centralizzazione.

IRR: un record `route`

```
route:          212.25.160.0/19
descr:          Seeweb srl
origin:         AS12637
mnt-by:         SEEWEB-MNT
created:        2006-02-09T08:08:36Z
last-modified:  2006-02-09T08:08:36Z
source:         RIPE
```

Autorizza AS12637 ad annunciare la rete `212.25.160.0/19`.

IRR: un record `as-set`

```
as-set:          AS12637:AS-CUSTOMERS
descr:           Seeweb and its IPv4 customers
members:         AS12637, AS31076, AS35131, AS6831,
                 AS50627, AS54103, AS204180
members:         AS12654 # RIPE RIS Routing Beacons
admin-c:         AB91-RIPE
tech-c:          SWBN-RIPE
mnt-by:          SEEWEB-MNT
created:         2006-11-24T23:44:15Z
last-modified:   2015-08-13T00:06:50Z
source:          RIPE
```

Elenca una serie di AS, ma inserirli qui non richiede autenticazione.

Domande?

`http://www.linux.it/~md/text/bgp-security-esc2k15.pdf`

(Google . . . Marco d'Itri . . . I feel lucky)