Bogons: Pacchetti IP con Indirizzi non Validi

Uno dei problemi che affliggono il traffico in internet è la presenza di pacchetti IPv4 falsi, ovvero nei quali è specificato un falso od illegale numero IP come sorgente. Spesso questi pacchetti sono chiamati *Bogons* e la loro origine è dovuta sia a macchine configurate male che a tentativi di attacchi. E' utile pertanto indicare quali numero IP sono validi e come fare a distinguerli. In questo articolo consideriamo il caso di una organizzazione la cui rete informatica è connessa a internet, in un prossimo articolo considereremo invece il problema dal punto di vista di un Internet Provider o Carrier.

E' ovvio che pacchetti con indirizzi IP non validi sono un problema sia perché utilizzano banda preziosa per il nostro traffico (se l'indirizzo sorgente non è valido è ovvio che in ogni caso non possiamo rispondere al mittente) sia perché sono spesso utilizzati come mezzo per portare attacchi in incognito alle nostre reti e macchine.

1. Classi di indirizzi IPv4

Gli indirizzi IPv4 sono numeri di 32 bit normalmente indicati con 4 cifre ognuna da 0 a 255 (ogni cifra corrisponde a 8 bit) come ad esempio il numero 5.6.7.8. Ogni numero IP è diviso in due parti, quella più significativa a sinistra detta di *network*, quella meno significativa a destra detta di *host*. Inizialmente la divisione era fatta in modo fisso, ma siccome in questo modo si sprecavano molti indirizzi IP è stato introdotta una notazione detta CIDR (Classless Inter-Domain Routing) che indica quanti bit a partire da sinistra formano la parte di network. Ad esempio 5.6.7.8/8 indica che i primi 8 bit, e perciò il numero 5 iniziale, è la parte di network mentre 6.7.8 è quella di host. Analogamente 3.4.5.6/24 ha 3.4.5 per il network e 6 per l'host. Normalmente la parte di network ha dagli 8 ai 24 bit (e viceversa per quella di host).

La parte di network è assegnata ad una organizzazione (azienda, internet provider ecc.) ed è la sola che è considerata quando i pacchetti transitano in internet dai processi ed algoritmi di *routing*. All'interno di una organizzazione invece è solo la parte di host che è utile a router, switch ecc. per consegnare il pacchetto alla macchina destinataria. Se ad una organizzazione è assegnata una classe /24, questa ha 256 indirizzi IP (meno 2) che può usare per le proprie macchine, mentre in una classe /8 ci sono poco più di 16 milioni di indirizzi.

Gli indirizzi IP sono gestiti al più alto livello dalla IANA (Internet Assigned Numbers Authority) che li ha divisi in vari gruppi a seconda dell'uso. Possiamo riassumere la suddivisione di IANA come segue:

1. indirizzi riservati a IANA per proprio uso privato
2. indirizzi utilizzabili all'interno di reti private, all'interno di host, per scopi di test ecc.
3. indirizzi assegnati ad una delle 4 (ad oggi) Regional Internet Registry (RIR) che a loro volta li dividono ed assegnano alle Local Internet Registry (LIR) che a loro volta li assegnano alle organizzazioni, aziende ecc. che li utilizzano
4. indirizzi temporaneamente non assegnati da IANA, RIR o LIR
5. indirizzi utilizzati per multicast

Ovviamente i primi due tipi di indirizzi non dovrebbero mai comparire in pacchetti in internet né come indirizzi sorgenti né di destinazione. Gli indirizzi multicast sono validi solo come indirizzi di destinazione e solo in reti che supportano multicast. Quindi gli unici indirizzi validi sia come sorgente che come destinazione sono quelli del terzo tipo. Il problema nel filtrare gli indirizzi non validi in internet risiede principalmente con gli indirizzi nel quarto punto. E' vero che IANA pubblica una lista delle assegnazione da lei fatte, ma la lista cambia e quindi bisogna tenersi aggiornati costantemente. Per quanto riguarda invece gli indirizzi non assegnati da RIR e LIR al momento non vi sono procedure precise per averne una lista completa. Per quanto riguarda i punti 1, 2 e 5 la lista è:[1]

- 0.0.0.0/8 (0.0.0.0 => 0.255.255.255) riservato IANA
- 10.0.0.0/8 (10.0.0.0 => 10.255.255.255) reti private
- 127.0.0.0/8 (127.0.0.0 => 127.255.255.255) interfacce interne di un host
- 169.254.0.0/16 (169.254.0.0 => 169.254.255.255) host che comunicano direttamente
- 172.16.0.0/12 (172.16.0.0 => 172.31.255.255) reti private
- 192.0.2.0/24 (192.0.2.0 => 192.0.2.255) per network di test (TEST-NET)
- 192.168.0.0/16 (192.168.0.0 => 192.168.255.255) reti private
- 198.18.0.0/15 (192.18.0.0 =>192.19.255.255) per benchmark test di reti
- 224.0.0.0/4 (224.0.0.0 =>239.255.255.255) multicast
- 240.0.0.0/4 (240.0.0.0 => 255.255.255.255) riservato IANA

2. Filtrare i Bogons

Per una organizzazione con una singola connessione ad internet non è difficile filtrare i Bogons sul router di accesso ad internet. Poiché vogliamo eliminare tutti i pacchetti in arrivo con un sorgente non valido, una vecchia *access-list* statica (packet-filter) è ancora la cosa più veloce e semplice. In Tabella 1 diamo un semplice esempio di un possibile

1 Le ultime due classi si possono accorpare in 224.0.0.0/3.

filtro per una rete interna con IP 3.4.5.0/24 da applicare all'interfaccia esterna del router per i pacchetti in ingresso da internet. Invertendo i FROM con i TO la stessa access-list può essere messa per i pacchetti in uscita dall'interfaccia esterna, questo per prevenire che i bogons possano uscire dalla nostra rete.[2] Alle reti citate in Tabella 1 si possono aggiungere quelle elencate da IANA e che si possono facilmente reperire in [3]. Ovviamente queste regole si possono anche mettere su una singola macchina su cui sia installato ad esempio un Personal Firewall.[3]

Un'alternativa all'uso delle access-list, che ha anche maggiori prestazioni, è data dall'uso di *route* nulle e filtri *reversed path* (RP). In molti router (ed alcuni firewall) esistono od è possibile creare delle interfacce virtuali *nulle*, tali che qualunque pacchetto ad esse inviato viene scartato, si vedano un paio di esempi in Tabella 2. Se pertanto nell'esempio in Tabella 1 mettiamo delle route verso una interfaccia nulla per tutte le reti dei primi 10 deny, escludendo 127.0.0.0/8 e 3.4.5.0/24, tutto il traffico verso questi indirizzi non attraverserà il router. In questo modo le access-list per i pacchetti in uscita dall'interfaccia esterna sono più semplici. A queste route possiamo aggiungere i filtri RP che sono spesso automaticamente attivati in router e firewall. Questi filtri eseguono un semplice controllo su ogni pacchetto in entrata nella macchina: scambiano l'indirizzo IP sorgente con quello di destinazione e verificano se secondo le route presenti nella macchina un tale pacchetto uscirebbe dalla interfaccia da cui è appena arrivato il pacchetto originale. In altre parole verificano che un possibile pacchetto di risposta segue la strada inversa del pacchetto originale. In caso contrario il pacchetto originale è scartato poiché proviene da una interfaccia sbagliata. Quindi unendo le route nulle ai filtri RP, pacchetti in arrivo con numeri IP sorgenti bogons sono scartati poiché le route nulle indicano che un eventuale pacchetto di ritorno uscirebbe da un'altra interfaccia, quella nulla, e non quella originaria. In questo modo possiamo ridurre anche le access-list in ingresso, a costo di aggiungere le route nulle ed utilizzare i filtri RP.

L'uso di route nulle e filtri RP ha però delle controindicazioni. Per prima cosa non vi è traccia nei log della macchina di tutti i pacchetti che vengono scartati in questo modo (l'interfaccia nulla è in pratica un buco nero). Inoltre per reti complesse, ad esempio con routing asimmetrico, non è possibile attivare i filtri RP poiché non è detto che il percorso di ritorno di un pacchetto sia esattamente l'opposto di quello di andata. Infine non è sempre semplice gestire le route nulle se si implementano processi di routing dinamico

2 Se si ha traffico multicast nelle regole in uscita bisogna usare 240.0.0.0/4 invece di 224.0.0.0/3.

3 In questo caso però bisogna stare attenti a non filtrare i pacchetti leciti delle reti 127.0.0.0/8 e 3.4.5.0/24.

quali BGP, OSPF ecc.

Andrea Pasquinucci
Consulente di Sicurezza Informatica
pasquinucci@ucci.it

Riferimenti Bibliografici

[1] IANA http://www.iana.org/assignments/ipv4-address-space
[2] Special-Use IPv4 Addresses, RFC-3330
[3] The Team Cymru Bogon Reference Page,
http://www.cymru.com/Bogons/index.html

```
# anti-spoofing
deny FROM 0.0.0.0/8 TO any
deny FROM 10.0.0.0/8 TO any
deny FROM 127.0.0.0/8 TO any
deny FROM 169.254.0.0/16 TO any
deny FROM 172.16.0.0/12 TO any
deny FROM 192.0.2.0/24 TO any
deny FROM 192.168.0.0/16 TO any
deny FROM 198.18.0.0/15 TO any
deny FROM 224.0.0.0/3 TO any
deny FROM 3.4.5.0/24 TO any
# protect our mail server
accept FROM any TO 3.4.5.6/32 tcp=25
deny FROM any TO 3.4.5.6/32
#default
accept FROM any TO 3.4.5.0/24
```

Tabella 1. ACL in ingresso su interfaccia esterna

```
# Linux
modprobe dummy
ifconfig dummy0 6.7.8.1 netmask 255.255.255.255\
  broadcast 6.7.8.1 up
route add -net 10.0.0.0 netmask 255.0.0.0 dev dummy0

#Cisco
ip route 10.0.0.0 255.0.0.0 Null0
```

Tabella 2. Esempi di configurazione di route nulle