THE ITALIAN RESEARCH & EDUCATION NETWORK

Consortium GARR

WG-SEC-DDoS

Gruppo di lavoro GARR di contrasto ai Distributed Denial of Service (DDoS)

Nino Ciurleo

Workshop GARR Roma, 06/04/2017

Lavoro di gruppo

- Partecipanti:
  - ~ 20 partecipanti
- Argomenti trattati:
  - Condivisione esperienze:
    - Best practice configurazioni di rete anti DDoS su sedi GARR
    - Raccolta di dati statistici sugli attacchi da e verso le sedi GARR
  - Monitoring ed elaborazione delle statistiche:
    - GINS DDoS Monitoring
    - Sistema di monitoring del blackholing e del flowspec
    - Elastic search per elaborare dati di traffico
    - Sensibilità dei dati di traffico
  - Strumenti:
    - Blackholing e flowspec
    - Traffic Diversion – Mirroring
  - Altro:
    - DDoS da IOT

Lavoro di gruppo

- Attività:
  - Video conferenze
    - mensili
  - Studio applicativi software:
    - Fastnetmon + Exabgp
  - Condivisione know-how
    - Questionario per la raccolta delle esperienze della comunità
  - Analisi dati
    - Netflow
    - Mirroring

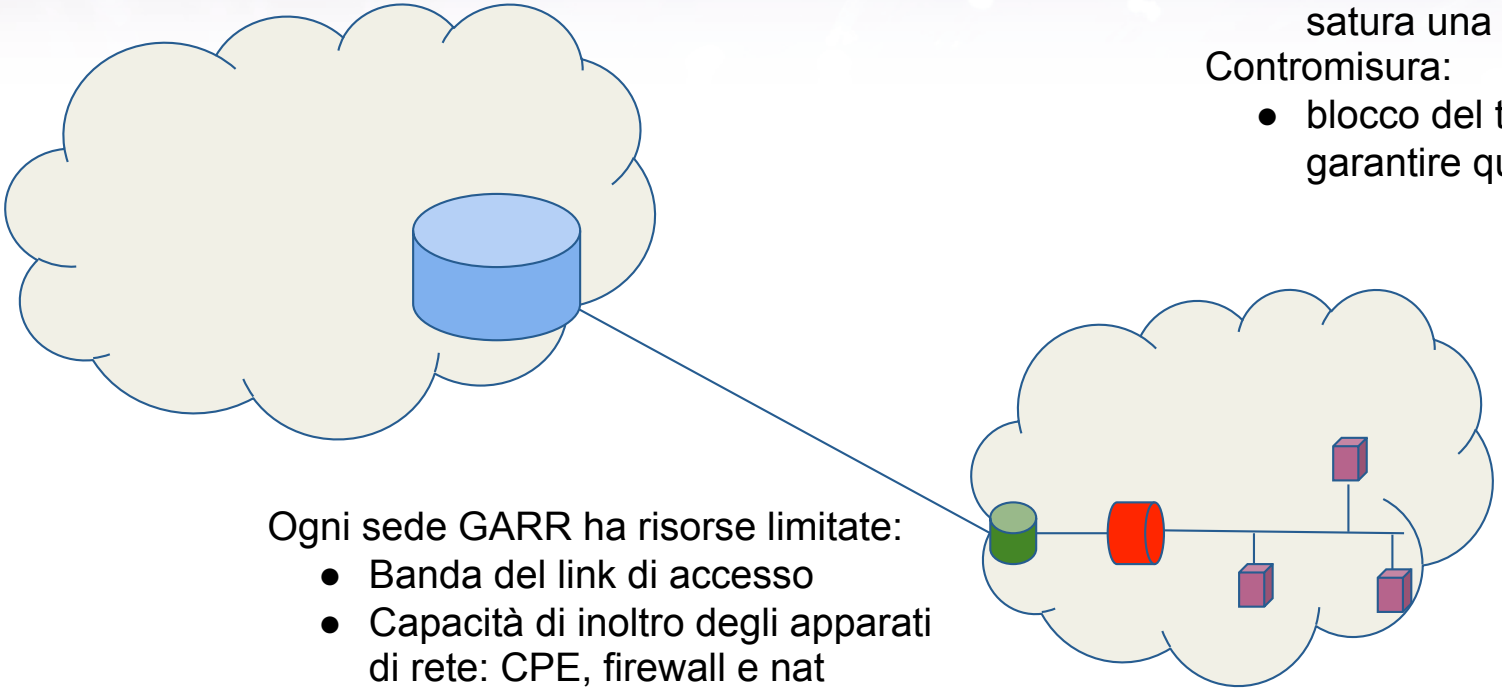
Cosa e' un DoS?

Attacco DoS:

- Traffico diretto verso uno o più host satura una delle risorse di rete

Contromisura:

- blocco del traffico malevolo ai fini di garantire quello lecito

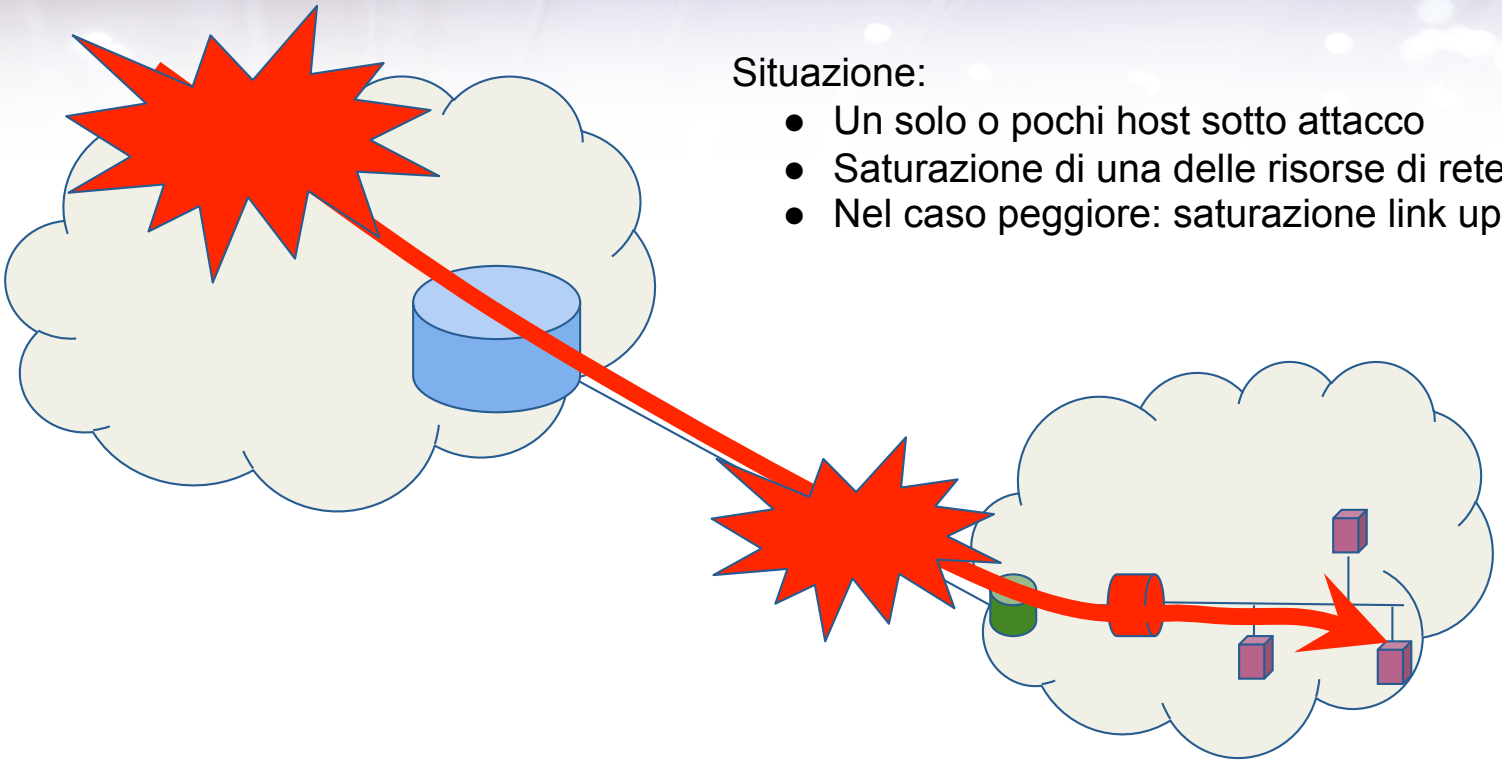


Ogni sede GARR ha risorse limitate:

- Banda del link di accesso
- Capacità di inoltro degli apparati di rete: CPE, firewall e nat

router
firewall/nat
host/box

Semplice contromisura: Blackholing

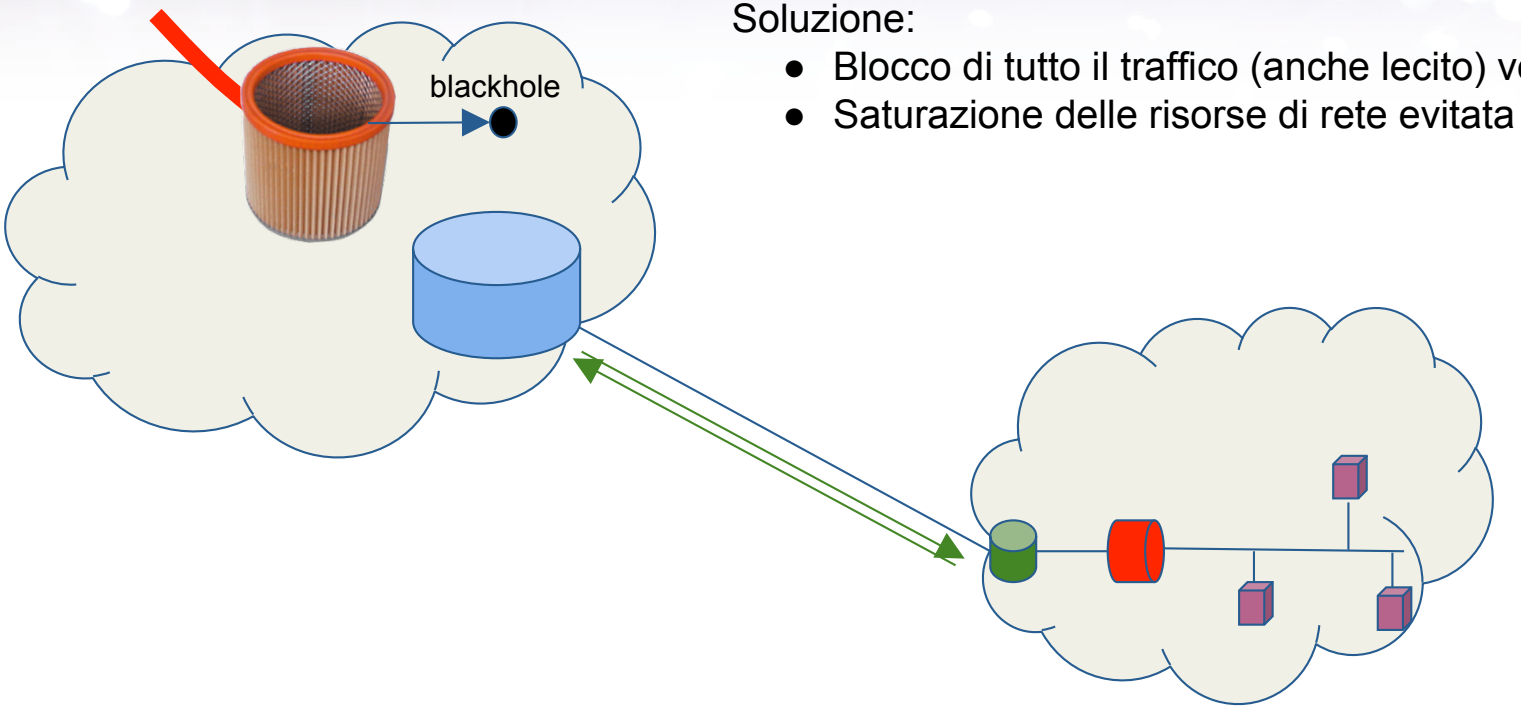


Situazione:

- Un solo o pochi host sotto attacco
- Saturazione di una delle risorse di rete isola la sede da GARR
- Nel caso peggiore: saturazione link upstream GARR

router
firewall/nat
host/box

Semplice contromisura: Blackholing



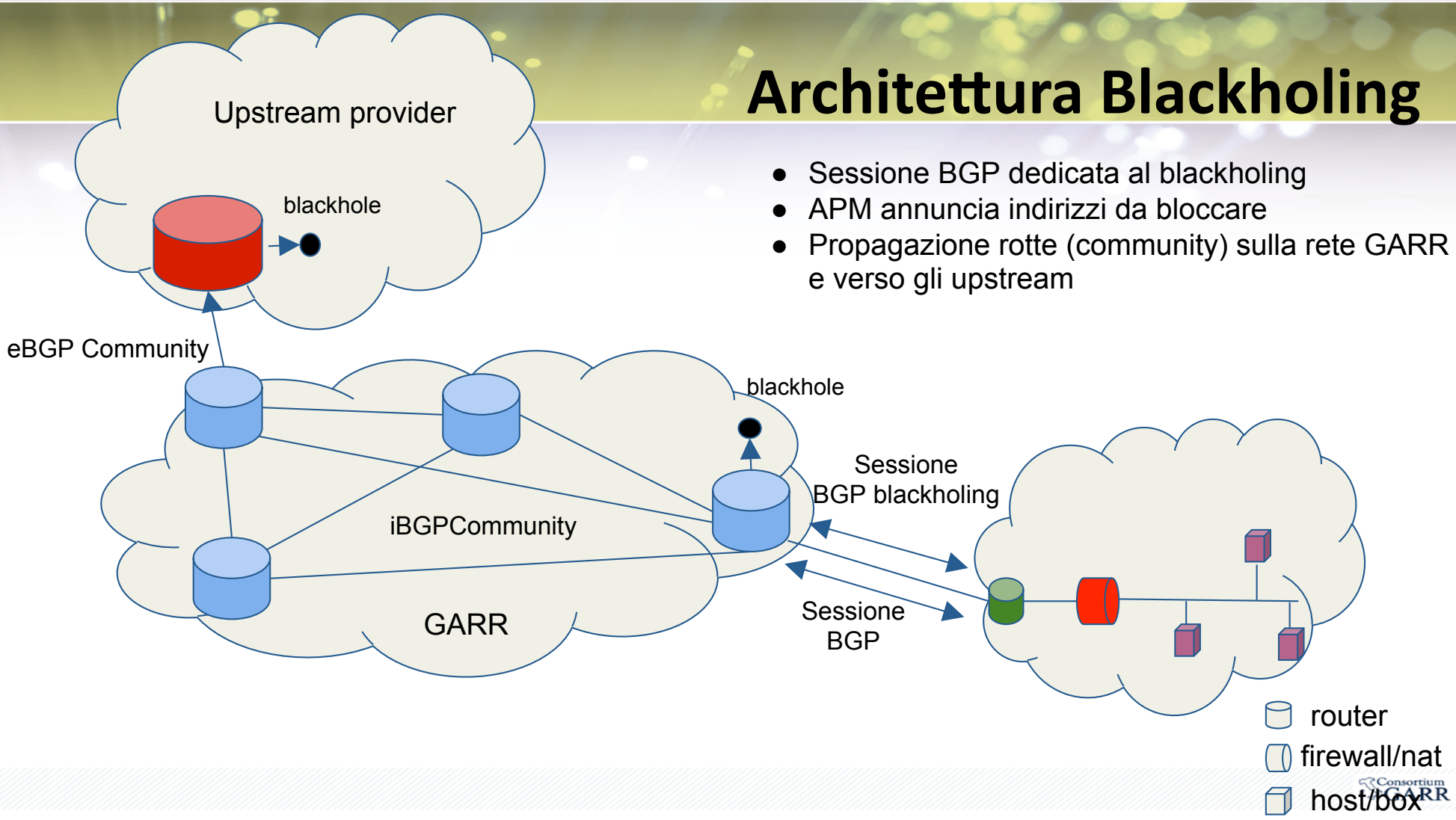
Soluzione:

- Blocco di tutto il traffico (anche lecito) verso l'host attaccato
- Saturazione delle risorse di rete evitata

router
firewall/nat
host/box

Architettura Blackholing

- Sessione BGP dedicata al blackholing
- APM annuncia indirizzi da bloccare
- Propagazione rotte (community) sulla rete GARR e verso gli upstream



Possibili implementazioni:

- Manuale:
  - Configurazione manuale annuncio BGP su CPE
- Automatica:
  - Detection dell'attacco automatica
  - Annuncio BGP automatizzato
  - Applicativi software:
    - Free Software (open source)
      - FastNetMon
    - Commerciali
      - Arbor network
      - Radware
      - …

Studio FastNetMon

- Lab presso Uni-Milano “Bocconi” (Marco Pirovano)
- Hardware:
  - HP ProLiant DL380 G6 E5540
    - 2 x 2.53GHz Quad Core
    - 24GB RAM
  - Scheda di rete 10G Intel X520-SR1 82599
- Software:
  - FreeBSD 11.0-RELEASE-p5
  - FastNetMon 1.1.3. (driver netmap)
  - InfluxDB 1.1.0

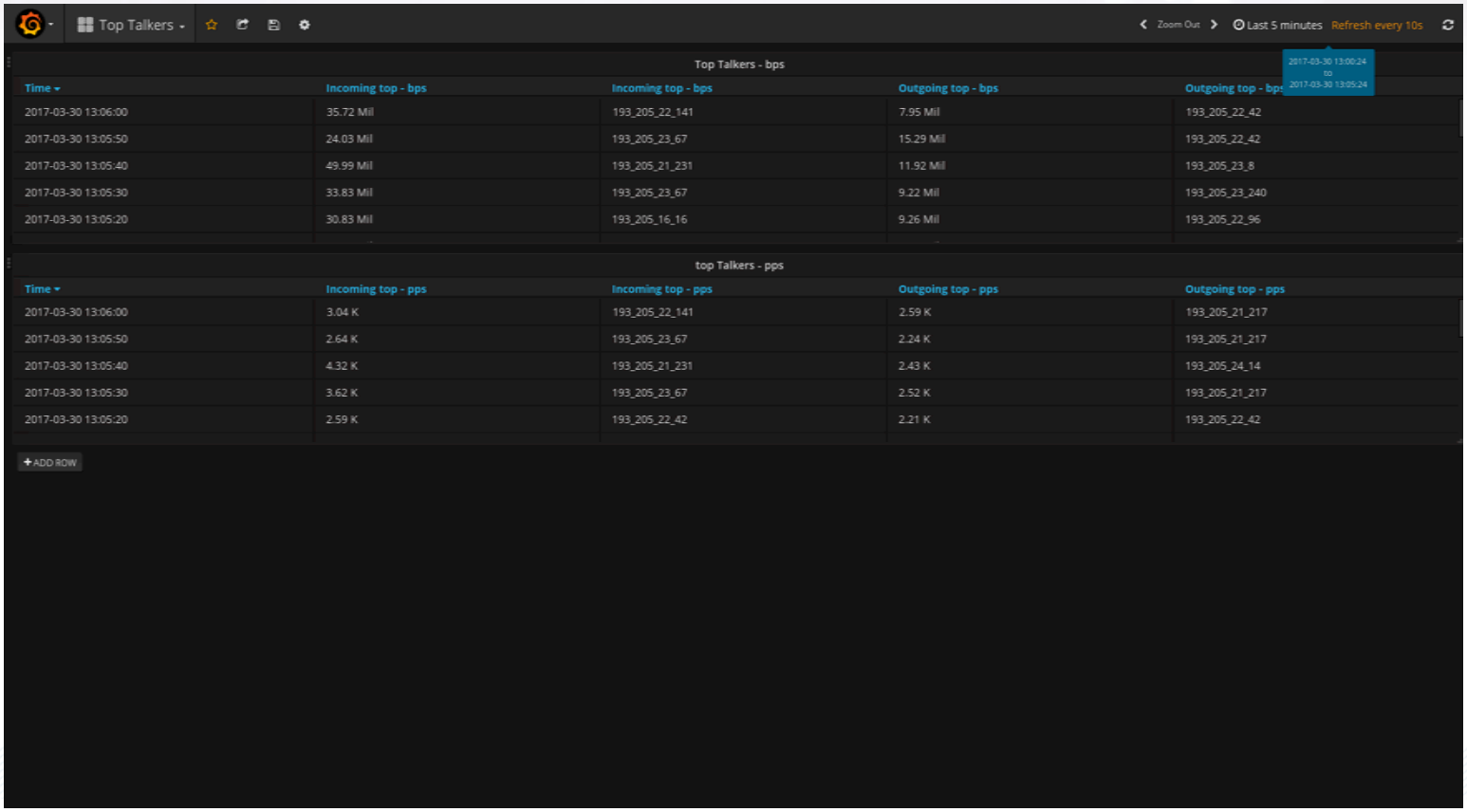
Studio FastNetMon

- Si basa su una semplice assunto:
  - Un solo indirizzo IP, di norma, non deve saturare tutte le risorse
  - Le risorse di rete sono finite e note (schede tecniche dei router/firewall) è quindi semplice scegliere le soglie di guardia
  - Whitelist per casi particolari: NAT, loadbalancer, etc
- Rilevamento basato su soglie:
  - Bandwidth
  - Packet per seconds (pps)
  - Flows per seconds (flows/s)
  - Generici o per protocollo:
    - TCP
    - UDP
    - ICMP
- Usato dalle NREN: deic e surfnet

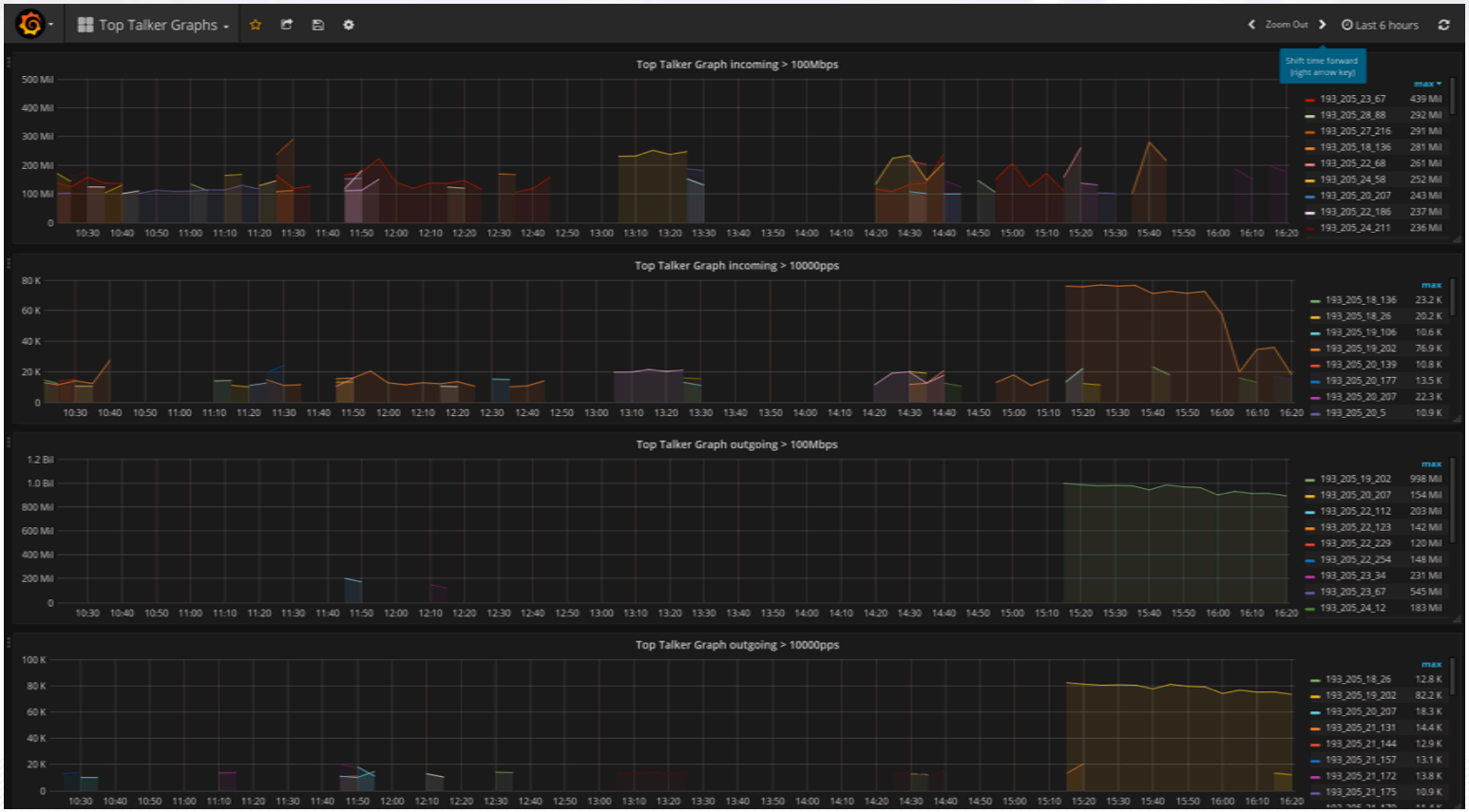
FastNetMon

Consortium GARR

FastNetMon


Top Talkers
Zoom Out
Last 5 minutes
Refresh every 10s
2017-03-30 13:00:24
to
2017-03-30 13:05:24
Top Talkers - bps
Time
Incoming top - bps
Incoming top - bps
Outgoing top - bps
Outgoing top - bps
2017-03-30 13:06:00 35.72 Mil 193_205_22_141 7.95 Mil 193_205_22_42
2017-03-30 13:05:50 24.03 Mil 193_205_23_67 15.29 Mil 193_205_22_42
2017-03-30 13:05:40 49.99 Mil 193_205_21_231 11.92 Mil 193_205_23_8
2017-03-30 13:05:30 33.83 Mil 193_205_23_67 9.22 Mil 193_205_23_240
2017-03-30 13:05:20 30.83 Mil 193_205_16_16 9.26 Mil 193_205_22_96
top Talkers - pps
Time
Incoming top - pps
Incoming top - pps
Outgoing top - pps
Outgoing top - pps
2017-03-30 13:06:00 3.04 K 193_205_22_141 2.59 K 193_205_21_217
2017-03-30 13:05:50 2.64 K 193_205_23_67 2.24 K 193_205_21_217
2017-03-30 13:05:40 4.32 K 193_205_21_231 2.43 K 193_205_24_14
2017-03-30 13:05:30 3.62 K 193_205_23_67 2.52 K 193_205_21_217
2017-03-30 13:05:20 2.59 K 193_205_22_42 2.21 K 193_205_22_42
+ ADD ROW

FastNetMon


Top Talker Graphs
Zoom Out
Last 6 hours
Top Talker Graph incoming > 100Mbps
Top Talker Graph incoming > 10000pps
Top Talker Graph outgoing > 100Mbps
Top Talker Graph outgoing > 10000pps

Esempio di attacco rilevato:

IP: 90.147.71.xx

- Attack type: udp_flood
- Initial attack power: 134450 packets per second
- Peak attack power: 134450 packets per second
- Attack direction: incoming
- Attack protocol: udp
- Total incoming traffic: 477 mbps
- Total incoming pps: 134450 packets per second
- Incoming udp traffic: 477 mbps
- Incoming udp pps: 133176 packets per second
- Incoming icmp pps: 1273 packets per second

Dettagli attacco rilevato:

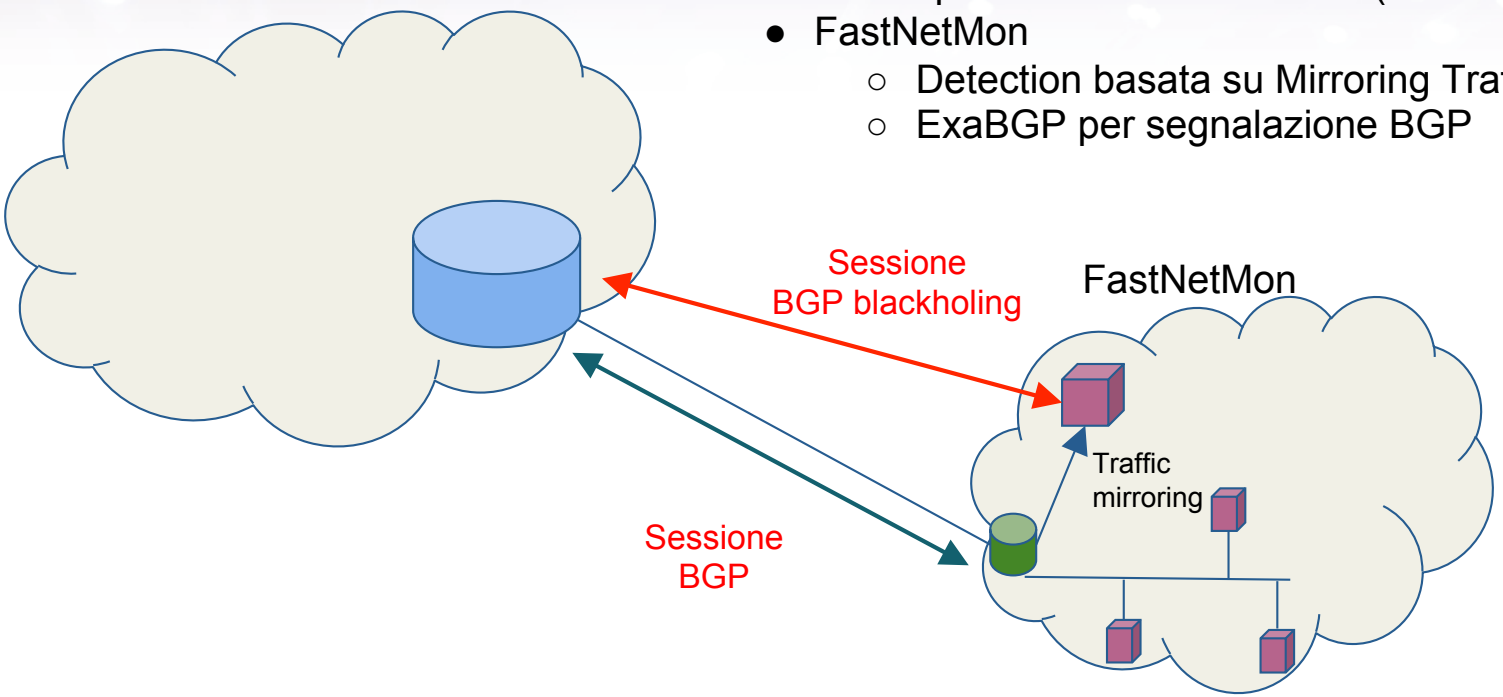
2017-03-10 18:46:14.849727 24.242.80.18:123 > 90.147.71.xx:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 52 sample ratio: 1
2017-03-10 18:46:14.849750 89.87.168.194:123 > 90.147.71.xx:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 52 sample ratio: 1
2017-03-10 18:46:14.849766 216.184.74.9:123 > 90.147.71.xx:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 57 sample ratio: 1
2017-03-10 18:46:14.849781 125.45.23.154:123 > 90.147.71.xx:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 36 sample ratio: 1
2017-03-10 18:46:14.849796 114.34.196.78:0 > 90.147.71.xx:0 protocol: icmp frag: 0 packets: 1 size: 70 bytes ttl: 243 sample ratio: 1
2017-03-10 18:46:14.849811 88.248.134.90:123 > 90.147.71.xx:39177 protocol: udp frag: 0 packets: 1 size: 410 bytes ttl: 42 sample ratio: 1
2017-03-10 18:46:14.849826 194.85.80.51:123 > 90.147.71.xx:40992 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 48 sample ratio: 1
2017-03-10 18:46:14.849841 80.95.184.130:123 > 90.147.71.xx:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 45 sample ratio: 1
2017-03-10 18:46:14.849855 183.234.216.18:123 > 90.147.71.xx:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 43 sample ratio: 1
2017-03-10 18:46:14.849870 183.234.216.18:123 > 90.147.71.xx:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 43 sample ratio: 1
2017-03-10 18:46:14.849885 85.131.152.210:123 > 90.147.71.xx:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 50 sample ratio: 1
2017-03-10 18:46:14.849900 65.116.97.190:123 > 90.147.71.xx:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 45 sample ratio: 1
2017-03-10 18:46:14.849915 125.45.23.154:123 > 90.147.71.xx:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 36 sample ratio: 1
2017-03-10 18:46:14.849929 80.95.184.130:123 > 90.147.71.xx:39177 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 45 sample ratio: 1
2017-03-10 18:46:14.849944 124.65.105.90:123 > 90.147.71.xx:22100 protocol: udp frag: 0 packets: 1 size: 482 bytes ttl: 36 sample ratio: 1

[78:19:F7:5B:30:01 -> 00:04:96:8F:B0:45] [IPv4][24.242.80.18:123 -> 90.147.71.xx:40992] [l3_proto=UDP][ip_fragmented: 0][hash=0][tos=0]
[tcp_seq_num=0] [caplen=482][len=482][parsed_header_len=0][eth_offset=0][l3_offset=14][l4_offset=34][payload_offset=42]

protocol: NTP master_protocol: Unknown

Scenario possibile: sistema di detection e blackhole automatizzato

- La tempestività è fondamentale (attacchi “potenti” < 5 min)
- FastNetMon
  - Detection basata su Mirroring Traffico o Netflow
  - ExaBGP per segnalazione BGP



router
firewall/nat
host/box

Scenario possibile:

- Monitoring delle sessioni BGP di blackholing
  - Informazioni sui blackhole attivi in rete per NOC, CERT e APM
  - Tempistiche
    - Data e ora inizio annuncio
    - Data e ora fine annuncio
  - Tipologia
    - solo su upstream
    - su upstream e interno a GARR

Fine

Contatti:

wg-sec-ddos@garr.it

nino.ciurleo@garr.it

https://wiki-wg-sec.garr.it