Consortium GARR

THE ITALIAN EDUCATION & RESEARCH NETWORK

Mitigazione dei DDoS: aggiornamento sulle attività

Nino Ciurleo

Workshop GARR 2019
Università di Roma Tre, 10/Ott/2019

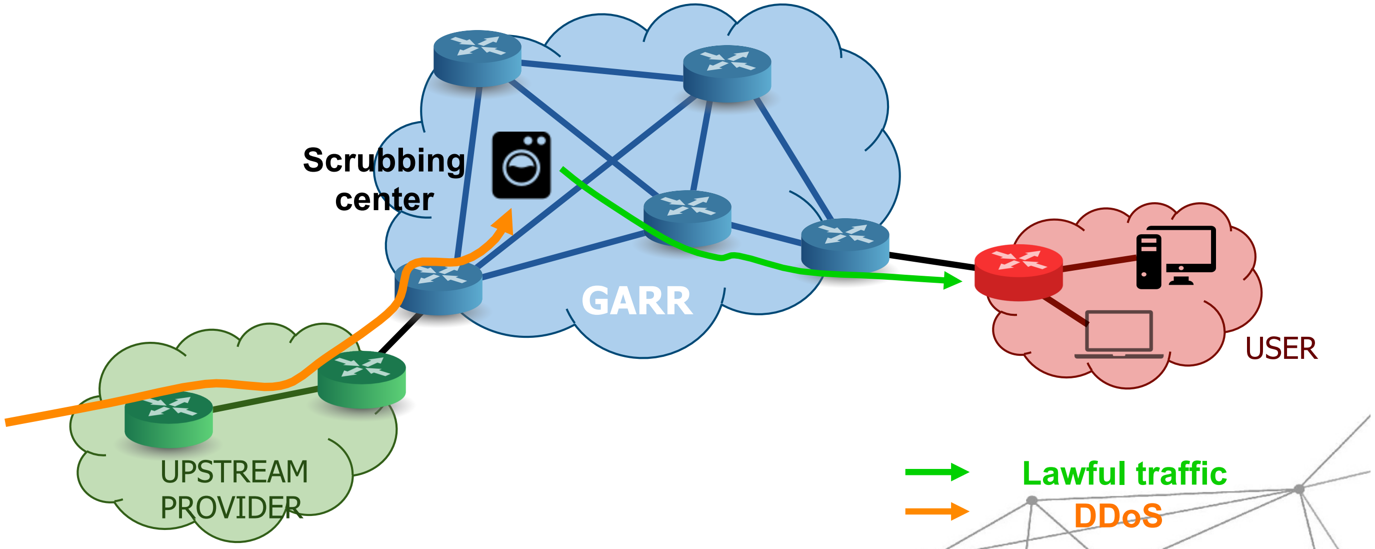
Scrubbing centers - dark side

- ***Managed* object** definition and management, a **constant effort**

- Attack traffic ***Diversion*** and clean traffic ***Re-injection*** need a constant update **effort on the whole network configuration** (VRF, tunnels, etc)

- A scrubbing center is **expensive** and represents a **single point of failure**

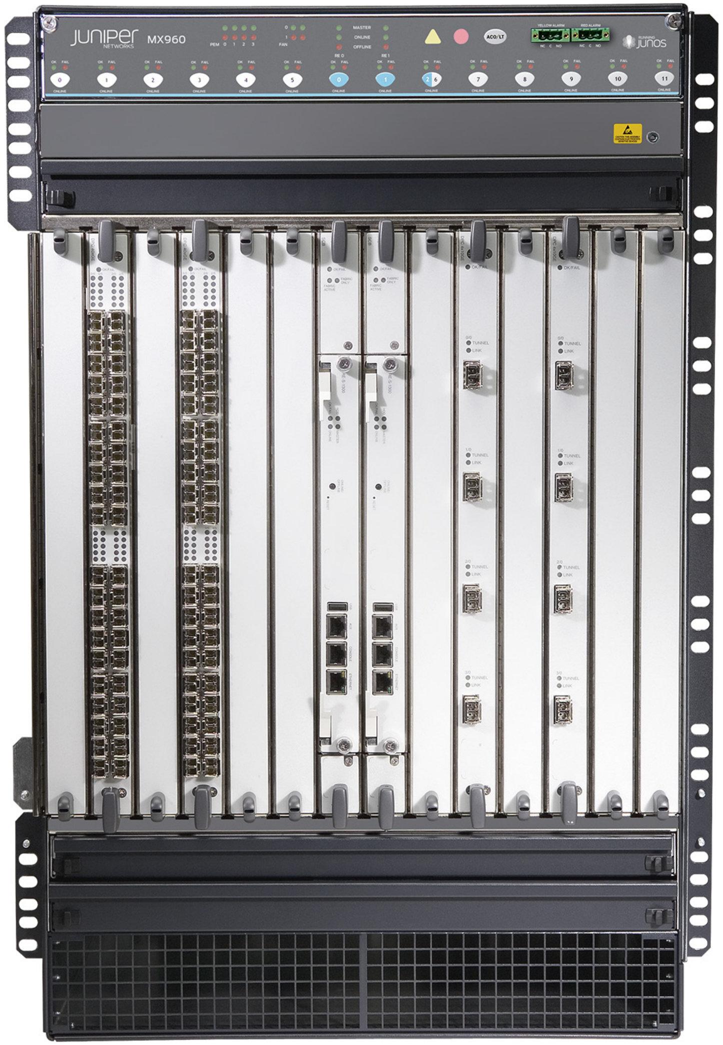
- **Scrubbing centers** are **black box**



Juniper integrated features

Juniper MX integrated features:

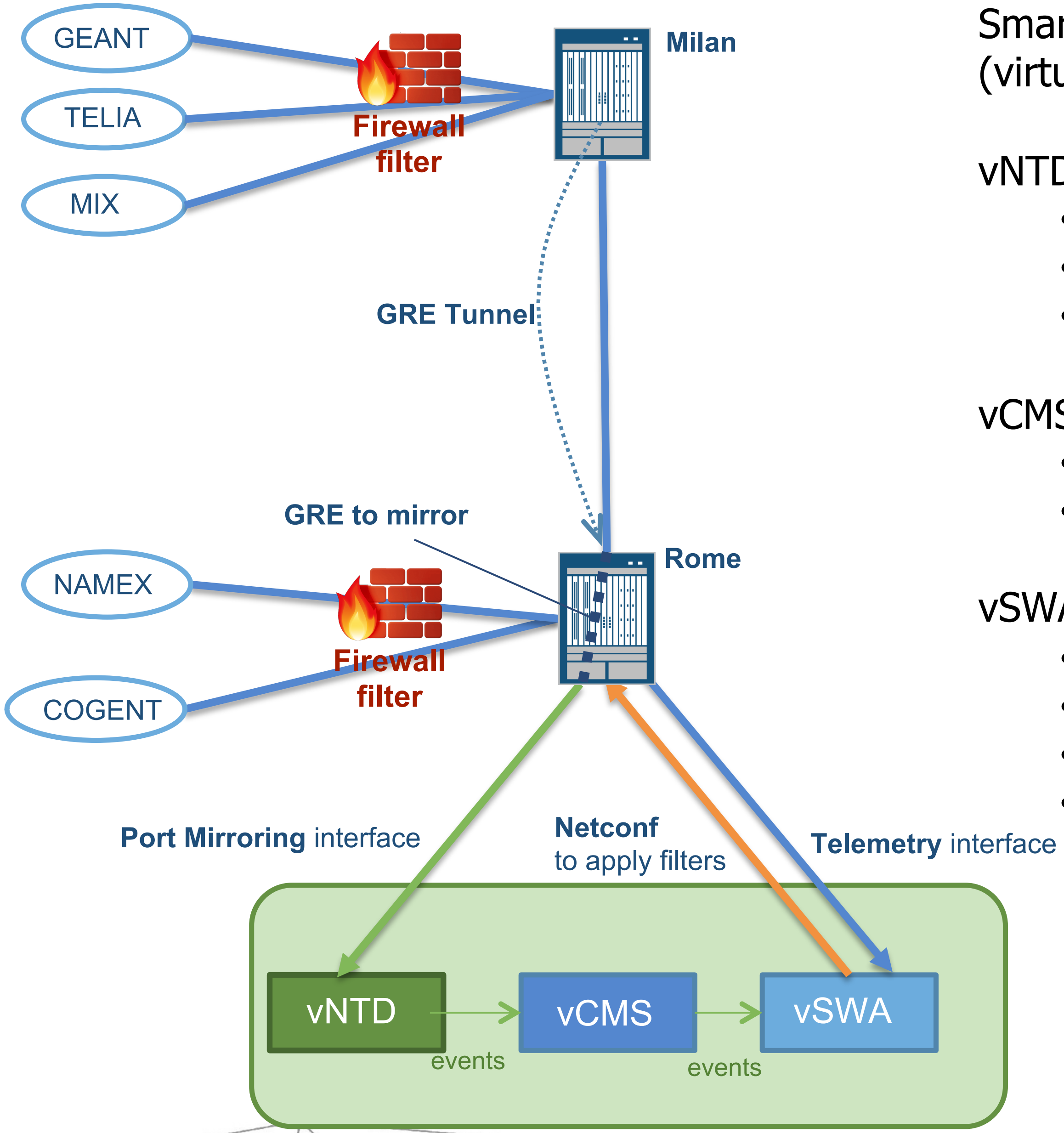
- MX **Trio chipset** capable for inline filtering
- **Telemetry** (filter traffic counters)
- Port-**Mirroring** (whole attack packet analysis)
- **Volatile** firewall **filters** (very fast)
- ***flexible-mask-match*** (payload matching filters)
- **NETCONF** interface (automation)



Corero approach

- Corero has a different type of DDoS engine:
  - Based on global ***rules*** that **triggering in the logic** that **define**, on the fly, **implementation filters** on Juniper nodes
  - SDN type slitting of:
    - **Logic** (Corero Smartwall TDD virtual machines)
    - **Filtering** (firewall filters on Juniper nodes).

Corero architectural components



Smartwall TDD from Corero is a software (virtual nodes)

vNTD - **Detection**

- Mirrored traffic capture
- LOG messages conversion
- More than on vNTD

vCMS - **Management**

- All system management
- *Rules* (eg. thresholds) configuration

vSWA - **Analisys and Mitigation**

- Attack traffic analysis
- Firewall filter **match rule creation**
- Filter application by NETCONF
- Web GUI:
  - Traffic statistics
  - Reports

Corero PoC first positive feedbacks

- **Very high scalability**, because of the advantage of Juniper features:
  - **Sampled** traffic mirroring (Detection)
  - *Flexible-match-mask* (Mitigation)

- **Fully Automated** and **distributed instant** filters
  - NETCONF
  - Ephemeral DB

- Modern and **extensible** toolset
  - Splunk based
    - Efficient search engine
    - Customizable dashboards
    - Lookup tables easy **correlation** with external sources

- **Well detected** and managed attacks:
  - Very fast detection and mitigation (seconds)
  - All recurrent large DDoS
  - Also less frequent attack packets (eg DDoS triggering packages through GARR hosts) managed
- Mitigation techniques
  - Rules **matches selectively** attacks packets only also on **payload** fields.
  - Filters behavior are **clearly explained**
- **Light** deployment
  - Virtual machines
  - Router based (potentially all the GARR nodes)
  - No Diversion/Re-injection needed
- **No user specific thresholds** (managed object) to be **mantained**
- Customizable/integrable system
  - Customizable GUIs

Questions?

Thank you

Nino Ciurleo nino.ciurleo@garr.it