

---

# Possible Ways of DDoS Mitigation: from Internal eXperience to Internet eXchange

Ben Li

(ex Technology VP of a Local IDC)

# DDoS Mitigation – Before Anything Else

---

## Detection of Attacks

- MRTG
  - SNMP
  - Log
  - NetFlow
-

## DDoS Mitigation – the Traditional Ways

---

- Set port speed 10; set duplex half
  - Unplug
  - Inform Upstream to filter IP (by email/phone/fax)
  - More specific route advertisement + Black hole (by BGP community)
-

## DDoS Mitigation as a Service

---

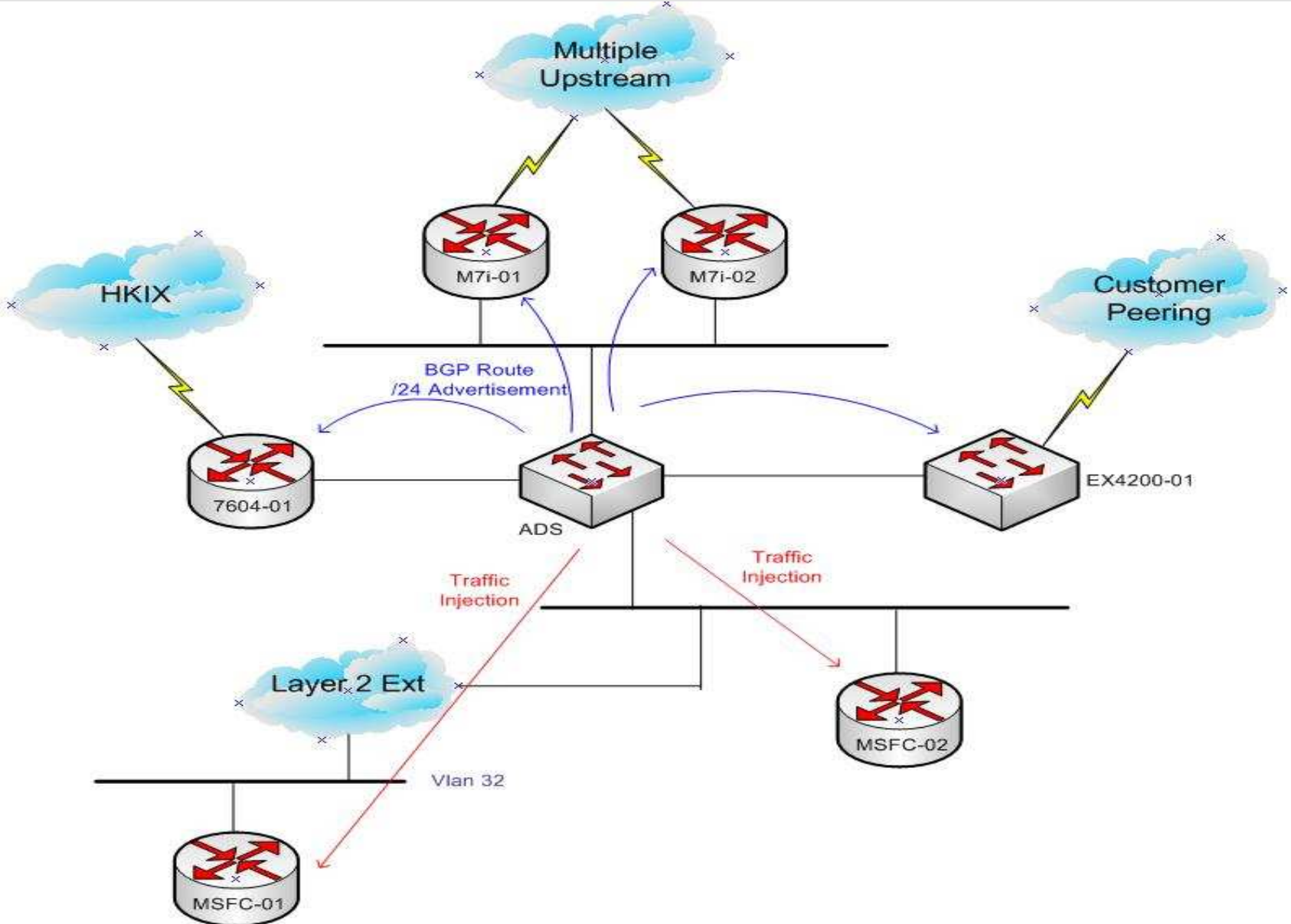
- ❑ Offered by an International IP Transit provider since 2008.
  - ❑ Traffic baseline monitored by provider.
  - ❑ Two connections (1 physical + 1 GRE) separating normal and “cleaned” packets.
  - ❑ Mitigation startup automatically or follow pre-agreed procedure.
  - ❑ Designed for enterprise users in mind.
  - ❑ Packet routing issue.
-

## Self Healing Solution

---

- ❑ For high packet rate & low volume attacks
  - ❑ For attacks through HKIX.
  - ❑ One ADS (Attack Defense System) device for all (3) centers.
  - ❑ ADS seat in parallel with core router and form BGP with all edge routers.
  - ❑ Manually advertise more specific route
-

# Self Healing Illustrative Diagram



# One Step Forward – Protection on the IX rim

---

- ❑ ADS put onto HKIX Layer-2 Platform and forming BGP peers with HKIX Route Servers. No routes would be advertised during normal situation.
- ❑ Other ISP incoming traffic to IDC go through normal paths.
- ❑ Flow Analyzer keep collecting NetFlow data from IDC's HKIX Routers and build baseline.
- ❑ All IDC HKIX Routers advertise routes in /22 or shorter.
- ❑ When DDoS attack happen, Flow Analyzer generates alert and provide information on destination IP being attacked.
- ❑ Engineer verified the alert and control ADS in HKIX to advertise /24 or longer route (ideally, /32 if the counter parts accept)
- ❑ Traffic to the segment (or IP) being attacked will be redirected to the ADS through BGP mechanism.
- ❑ Attacking packets will be dropped by the ADS and the clean traffic will be redirected, through the pre-established GRE tunnel, to another IDC HKIX Router.
- ❑ When DDoS attack stop, the more specific route will then be removed from the ADS and all traffic flow resumed.

# IX Protection Illustrative Diagram

