DDoS Mitigation Offload: A DOTS Applicability Use Case

draft-hayashi-dots-dms-offload-usecase

Yuhei Hayashi / NTT

Kaname Nishizuka / NTT Communications

Mohamed Boucadair / Orange

Prague, IETF#104, March 2019

Agenda

- Why an Applicability Document?
- A simplified design
- Demonstrating the proposal

Why an Applicability Statement Document?

- Identify innovative deployment schemes to motivate the use of DOTS
  - Optimized scrubbing invocation
  - Distribute filtering enforcement

- Specification documents do not dwell on deployment considerations
  - Providing informational documents is helpful to see DOTS a deployment reality

A Simplified Proposal

- Collaboration DMS, orchestrator, and forwarding nodes
- Withdrawing our expansion of signal channel for the moment
  - To reconsider requirement for expanded signal / data channel

Component Diagram

```
+--------------+        +-----------+
|              |        | DDoS      |+
| Orchestrator |<-------| mitigation||
|              |S DOTS C| systems   ||
+--------------+        +-----------+|
       |                  +----------+
       | e.g., BGP, BGP Flowspec
       |
       |  +------------------+
       +->| Forwarding nodes |+
          +------------------+|
           +------------------+
    * C is for DOTS Client function
    * S is for DOTS Server function
```

Sequence Diagram

```
+------------+         +----------+   +------------+
|            |         |DDoS      |+  | Forwarding |+
|Orchestrator|         |Mitigation||  | Nodes      ||
|            |         |Systems   ||  |            ||
+------------+         +----------+|  +------------+|
     |                  +----------+   +------------+
     |                        |              |
     | DOTS Request           |              |
     |S<-------------------C|              |
     |                        |              |
     | e.g., BGP, BGP Flowspec |              |
     | Filter Attack Traffic  |              |
     |------------------------|------------->|
     |                        |              |
     * C is for DOTS Client function
     * S is for DOTS Server function
```

□ Different point from that of DDoS Orchestration usecase in current usecase draft

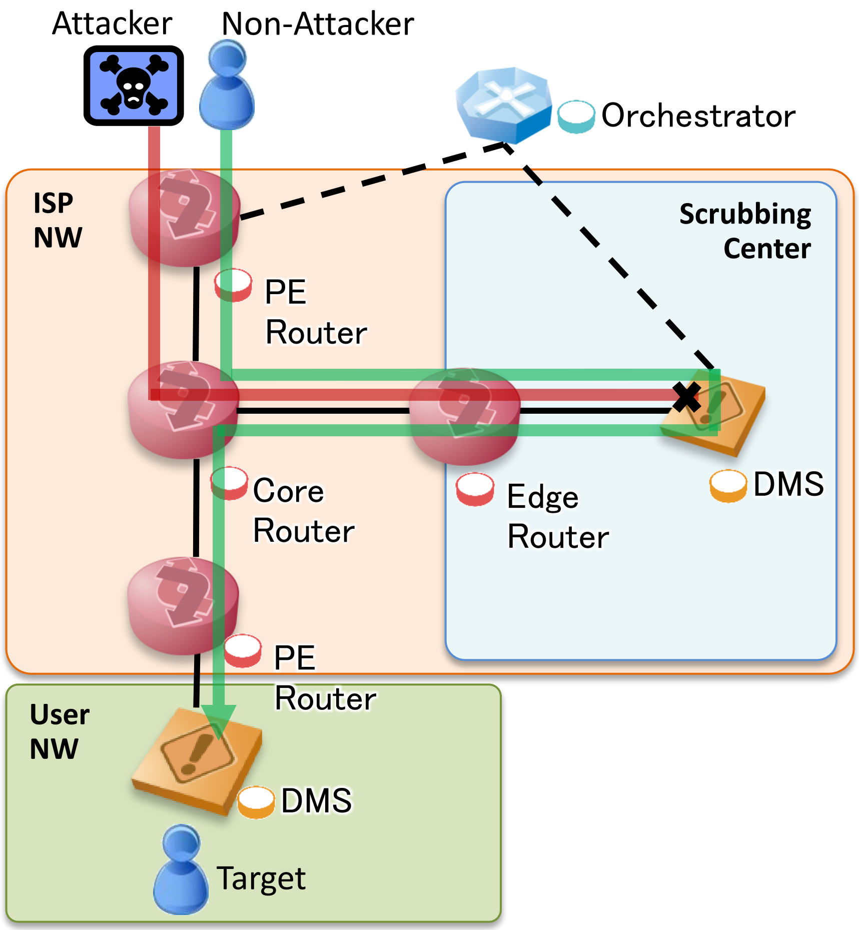
1st Applicability Case

- Case : DOTS Request via Out-of-band Link
- Case : DOTS Request via In-band Link

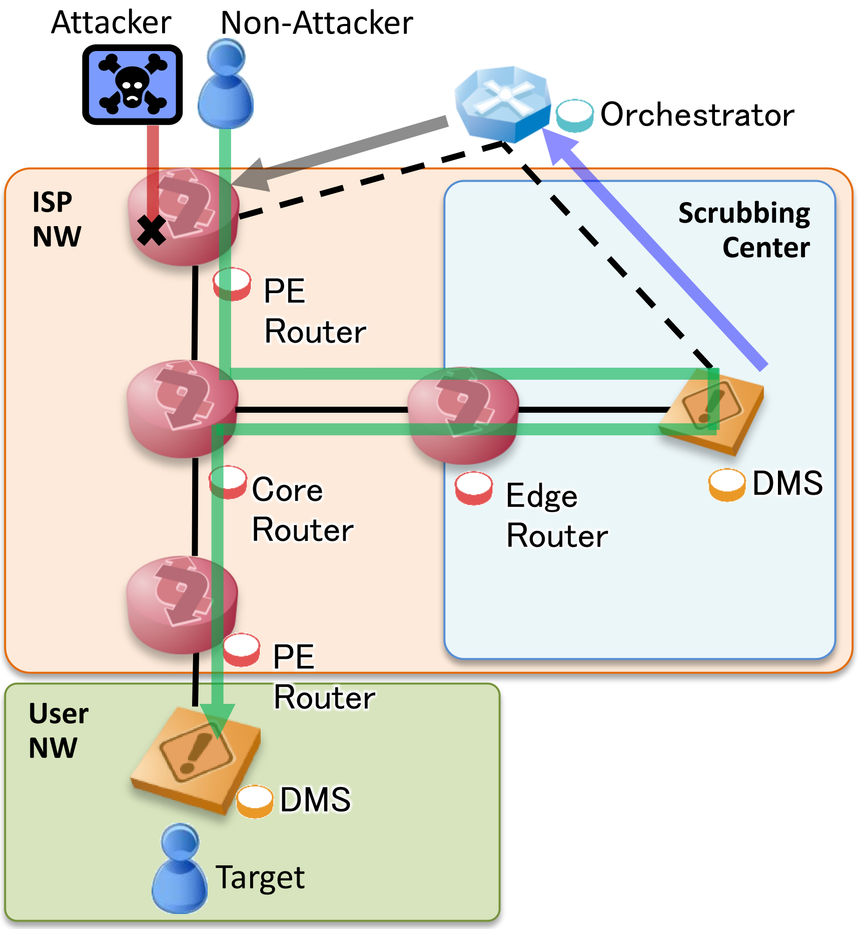
DOTS Signal : Data Channel

- 🟩 Normal Traffic
- 🟥 Attack Traffic
- 🟪 syslog
- 🟦 DOTS Signal
- ⬛ Filter Signal
- ─ In-band link
- - - Out-of-band link

Before



After



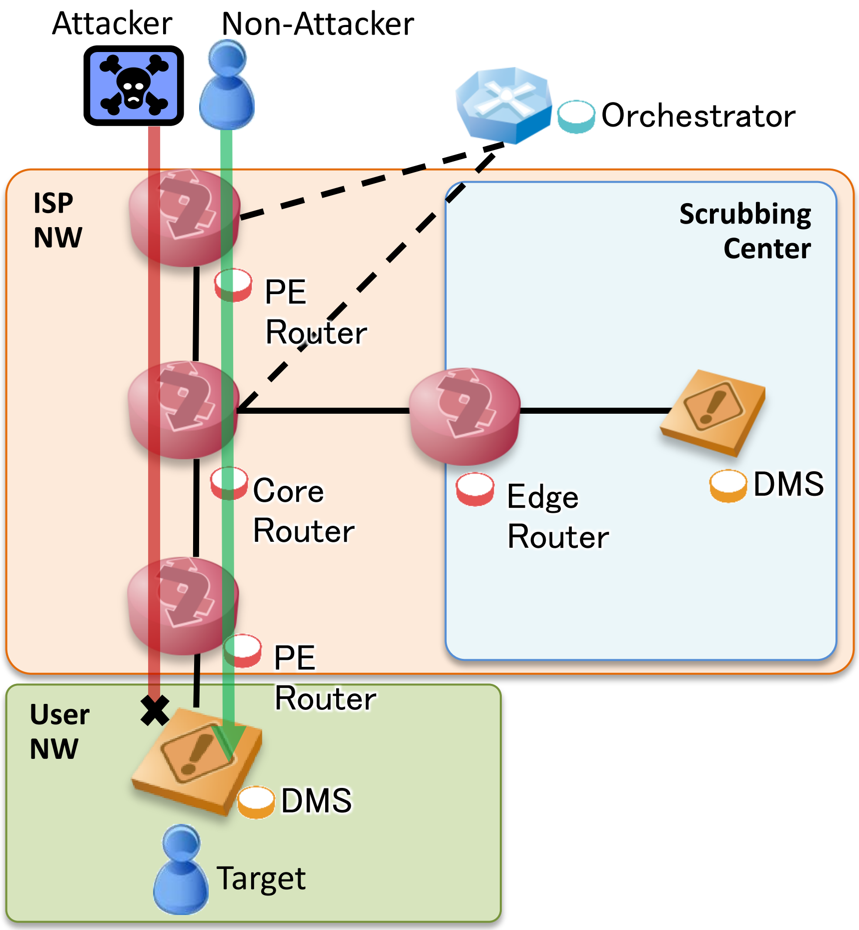
2nd Applicability Cases

- Case : DOTS Request via Out-of-band Link
- Case : DOTS Request via In-band Link

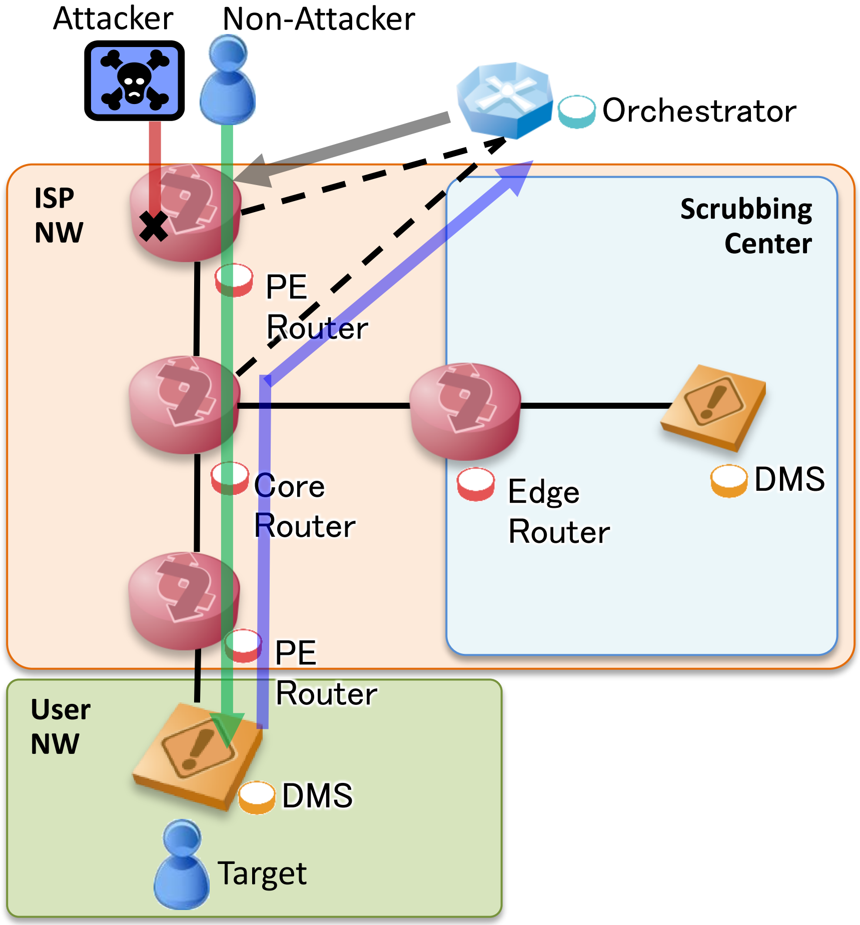
  DOTS Signal : Signal Channel

🟩 Normal Traffic
🟥 Attack Traffic
🟪 syslog
🟦 DOTS Signal
⬛ Filter Signal
— In-band link
- - - Out-of-band link

Before



After



Motivation of using DOTS

Case : DOTS Request via Out-of-band Link

・ ACL YANG model [rfc8519] cannot send information about identification of DOTS client’s request.
e.g. Orchestrator can identify DMS’s offload request by “cuid” in Data Chanel Signaling.

Case : DOTS Request via In-band Link

・In attack time, link is congested.

A PoC: Out-of-band Link

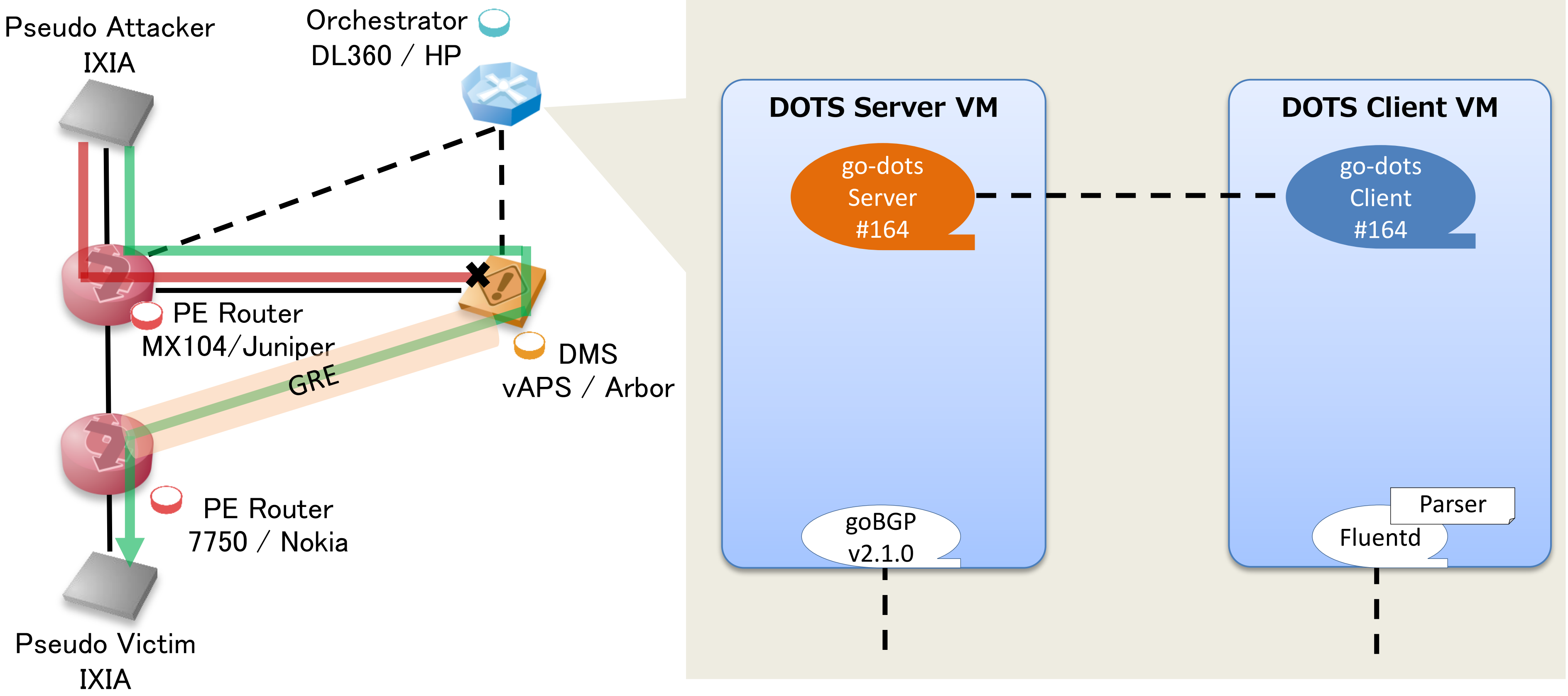
Situation

- DNS amp attack hits a network.

  Target’s IP addr : 10.0.0.1/32

  Attacker’s IP addr : 20.0.0.3/32

- Target’s traffic is already mitigated by a DMS.

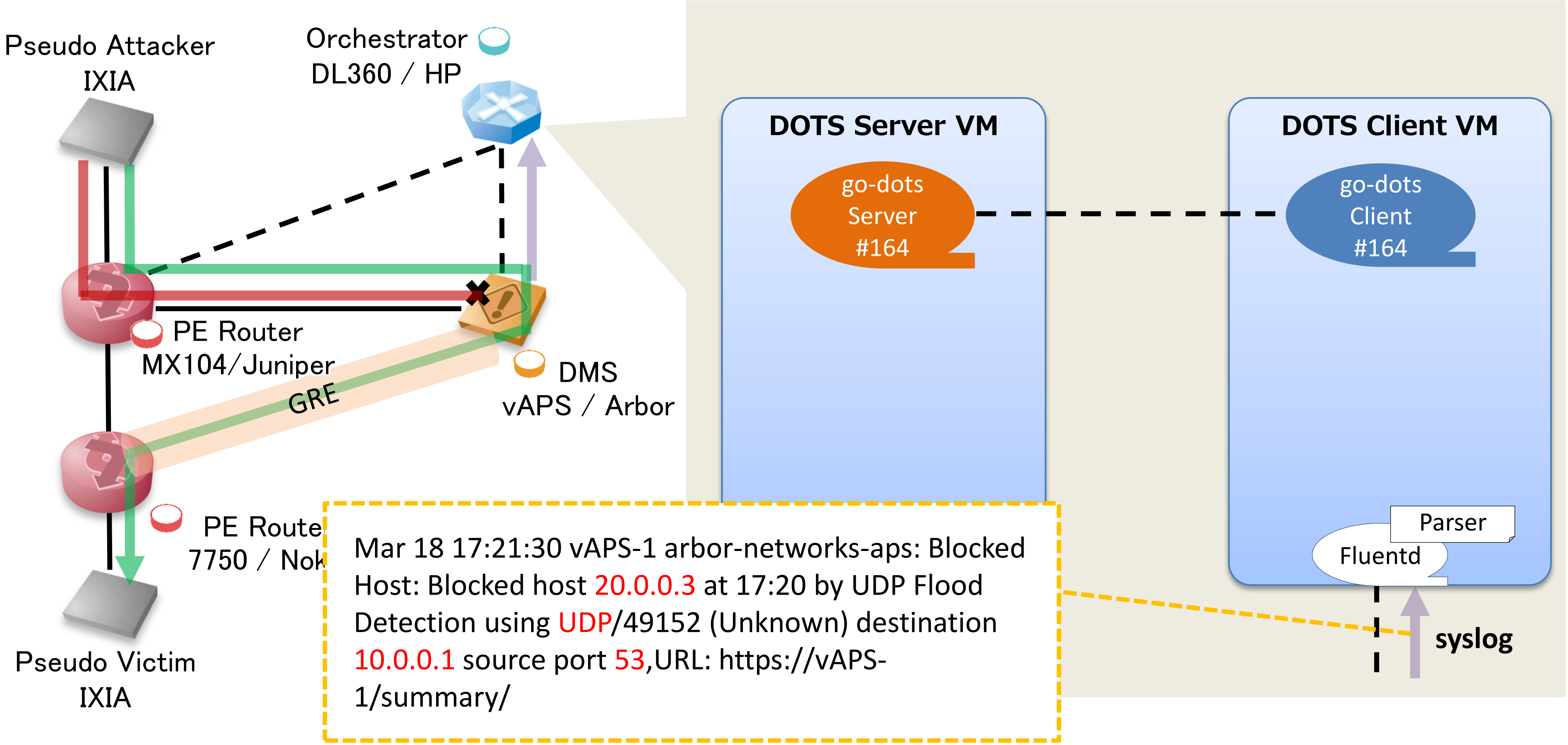


A PoC: Out-of-band Link

Action

- DOTS client extracts information of blocked traffic from syslog of DMS.

🟩 Normal Traffic
🟥 Attack Traffic
syslog
DOTS Signal
Filter Signal
In-band link
Out-of-band link



```
Mar 18 17:21:30 vAPS-1 arbor-networks-aps: Blocked
Host: Blocked host 20.0.0.3 at 17:20 by UDP Flood
Detection using UDP/49152 (Unknown) destination
10.0.0.1 source port 53,URL: https://vAPS-
1/summary/
```

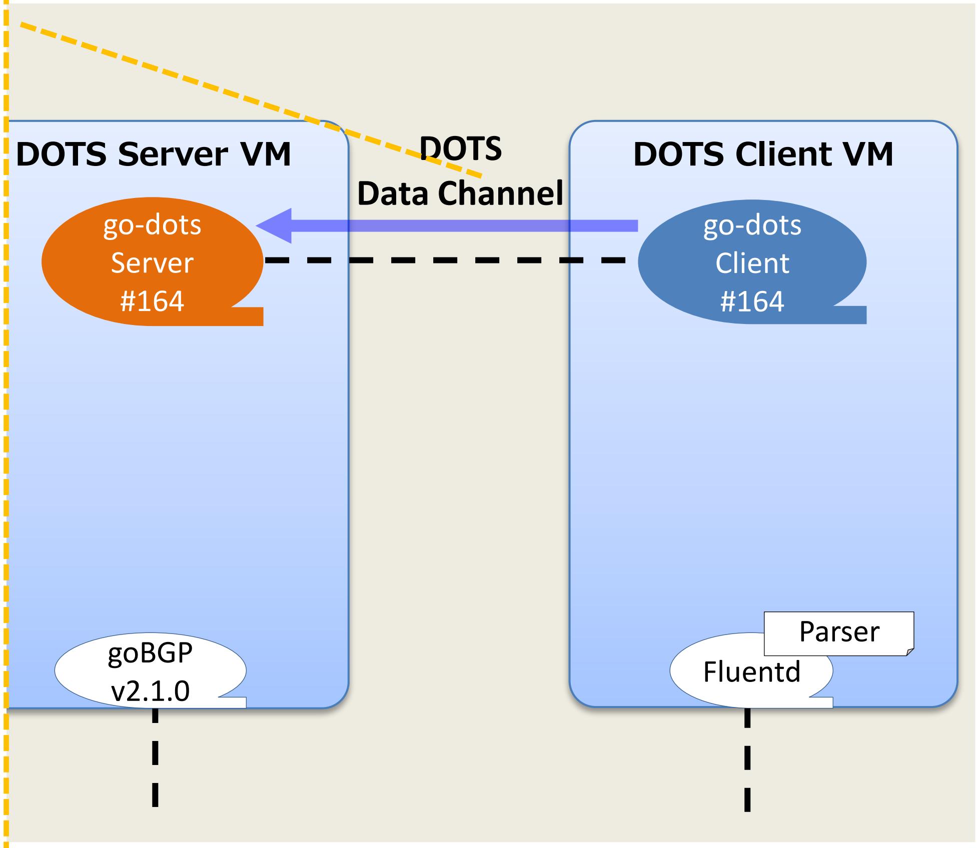
A PoC: Out-of-band Link

```
"ietf-dots-data-channel:acls": {
 "acl": [
  {
   "name": "MitReqAcl_000000108",
   "type": "ipv4-acl-type",
   "activation-type": "immediate",
   "aces": {
    "ace": [
     {
      "name": "dmsOffloadAceDrop_20.0.0.3",
      "matches": {
       "ipv4": {
        "destination-ipv4-network": "10.0.0.1/32",
        "source-ipv4-network": "20.0.0.3/32",
        "protocol": 17
       },
       "udp": {
        "source-port": {
         "operator": "eq",
         "port": 53
        }
       }
      },
      "actions": {
       "forwarding": "drop“
      …
```

Action

- DOTS client sends traffic information blocked by DMS.

← Normal Traffic
← Attack Traffic
← syslog
← DOTS Signal
← Filter Signal
—— In-band link
- - - Out-of-band link

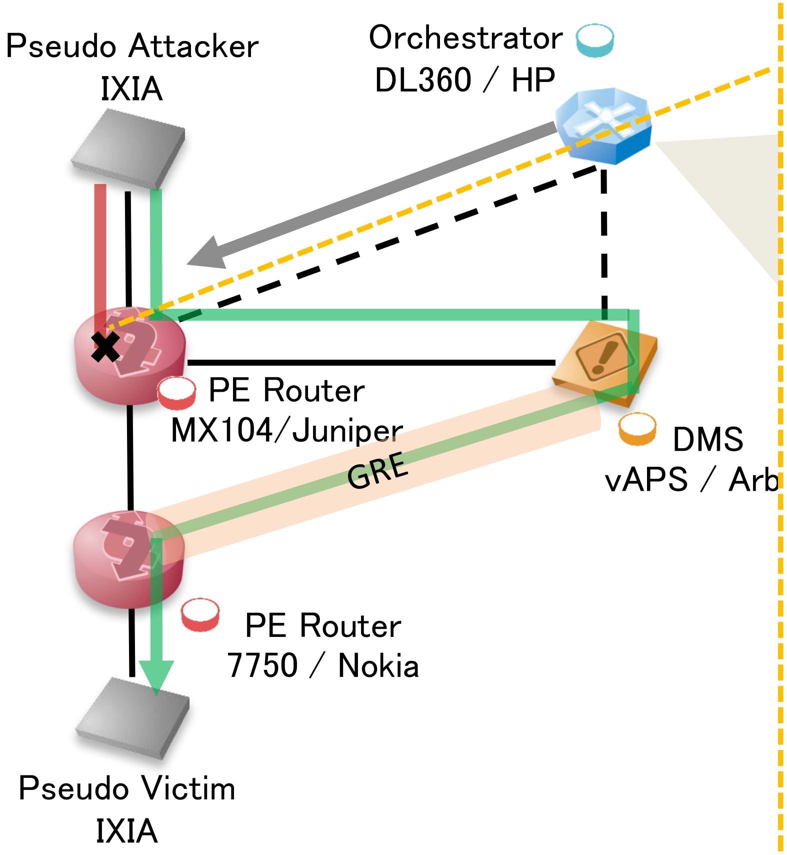


A PoC: Out-of-band Link

Normal Traffic
Attack Traffic
syslog
DOTS Signal
Filter Signal
In-band link
Out-of-band link

Action

- Go-bgp sends bgp flowspec to set PE router filter config.



```
10.0.0.1,20.0.0.3,proto=17,srcport=53/term:2
*BGP    Preference: 170/-101
          Next hop type: Fictitious, Next hop index: 0
          Address: 0x61f0910
          Next-hop reference count: 4
          Next hop:
          State: <Active Int Ext SendNhToPFE>
          Local AS:   100 Peer AS:   100
          Age: 14:40
          Validation State: unverified
          Task: BGP_100.50.0.0.73
          Announcement bits (1): 0-Flow
          AS path: I
          Communities: traffic-rate:0:0
          Accepted
          Localpref: 100
          Router ID: 50.0.0.73
```

What is Next?

- Received comments were addressed
- It is import to document applicability statements to help see DOTS a deployment reality
- Request the WG to consider adoption