DOTS Signal Channel Call Home: Updates since IETF#104 Prague

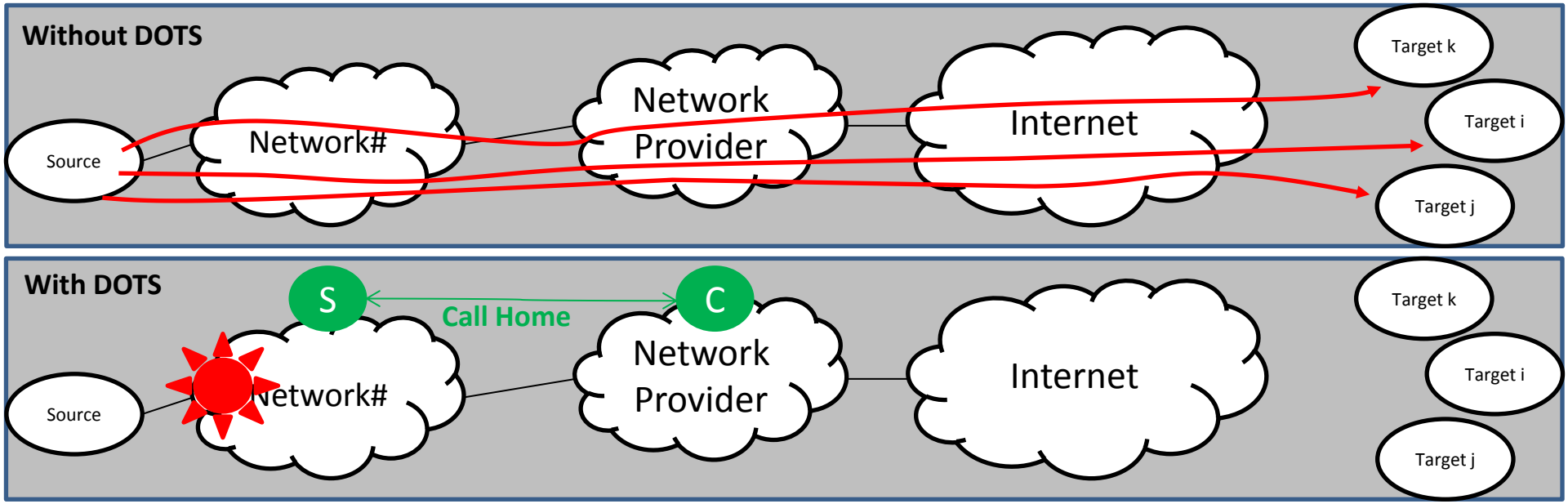
draft-ietf-dots-call-home

IETF#105 Montreal, July 2019

T. Reddy, M. Boucadair, J. Shallow

Scope

- The Call Home functionality is not specific to home networks
  - It applies each time there is a need to filter an attack near the sources (DC, Enterprises, …)
  - Added text to further clarify the scope



DOTS Extensions

- The following new attributes are defined
  - source-prefix, source-port-range, and source-icmp-type-range
- These attributes can be used in the signal channel even if the Call Home functionality is not enabled
  - Optional attributes for the base DOTS spec
- When used in the Call Home, source-prefix is a mandatory attribute

Dedicated Heartbeat Mechanism

- DOTS clients retrieve the session configuration parameter from DOTS servers
  - The DOTS server adjusts the heartbeat interval to accommodate binding timers used by on-path NATs and firewalls
- The DOTS client sends its HB immediately after the receipt of one from the DOTS server (to make use of fresh NAT/FW mappings)
- When an outgoing attack that saturates the outgoing link from the DOTS server is detected and reported by the DOTS client, the latter must continue to use the signal channel even if no traffic is received from its peer
- If the DOTS server receives traffic from the DOTS client, the DOTS server must continue to use the signal channel even if the missing heartbeat allowed threshold is reached
- If the DOTS server does not receive any traffic from the peer DOTS client (including replies to its HBs, the DOTS server must try to resume the (D)TLS session, not the DOTS client as (D)TLS initiation is reversed

Request Validation

- Only immediate mitigation requests are allowed
  - Requests with 'trigger-mitigation' set to false must be discarded by DOTS servers
- Validating prefixes
  - source-prefix must be within the scope of DOTS server domain
  - By default, any routeable prefix included in the target-prefix is considered as within the scope of the DOTS client

Misc

- Added some text about triggers at the DOTS client to initiate Call Home requests
- Disambiguate base DOTS signal vs. Call Home
  - Add an appendix to record the design rationale (thanks, Wei Pan)
- Re-structure the NAT/CGN text

What's Next?

- No issue is pending
- The content is stable
  - Request WGLC