Inter-Domain DOTS Use Cases

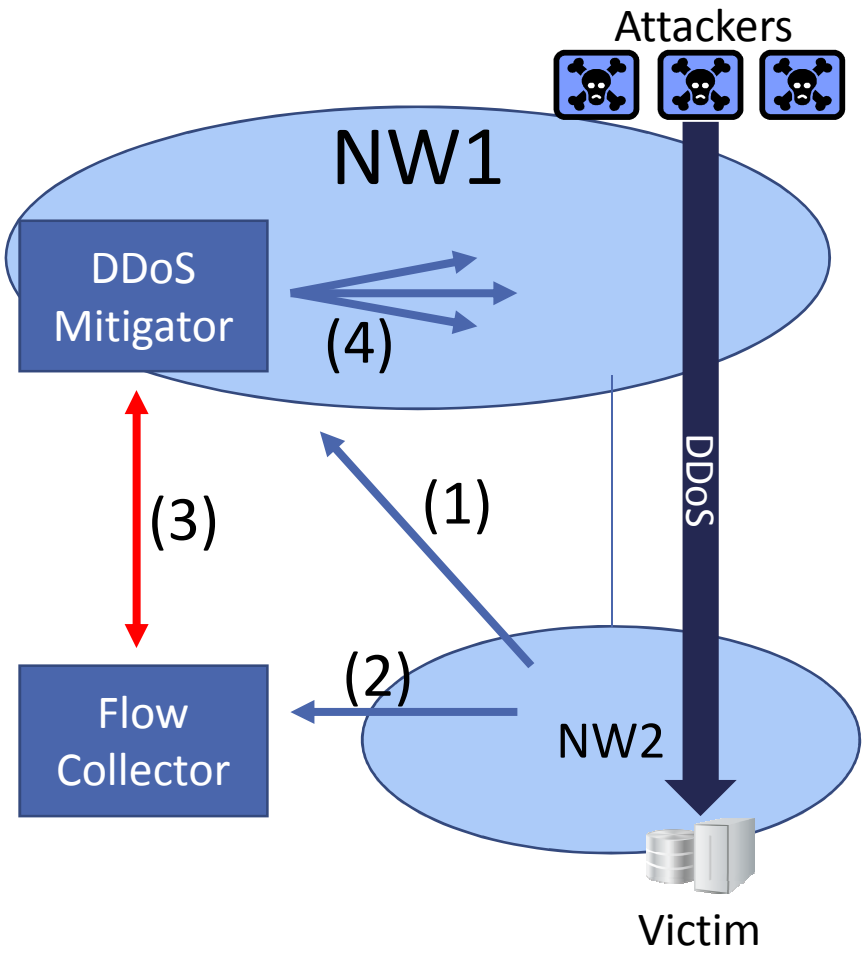
draft-nishizuka-dots-inter-domain-usecases-00

Kaname Nishizuka, NTT Communications
Nov. 2015 IETF94@yokohama

Draft Overview

- Motivation
  - The volume of DDoS attack will exceed available anti-DDoS capability by one organization.
  - Inter-domain cooperative DDoS mitigation is essential.
- Describe DDoS protection scenario in two stages
  - Provisioning stage & Signaling stage
  - Based on our production DDoS protection service
  - Willing to generalize it to be more vendor-agnostic to fit to DOTS.
- Describe three Inter-domain usecases

Scenario Overview



(1)Provisioning stage

Provisioning of DDoS protection capability

(2) DDoS Detection

- Automatic detection
- Automatic/manual trigger of DDoS protection

Scope of Dots

(3)Signaling stage

"Call for help" signaling from supplicant (=flowcollector, in our case) to DDoS mitigator

(4)Mitigation action from the mitigator to NW elements

- BGP injection(RTBH/Diversion)
- Controlling multi-vender mitigation box
- Changing ACL of routers
- Flowspec advertisement

Provisioning Stage

What information should be confirmed between DDoS mitigator and supplicant in advance?

1. Protection capability
2. Restriction on the range of IP addresses and ports
3. Return path information of the mitigated traffic
4. Authorization information to restrict the supplicant

Signaling Stage

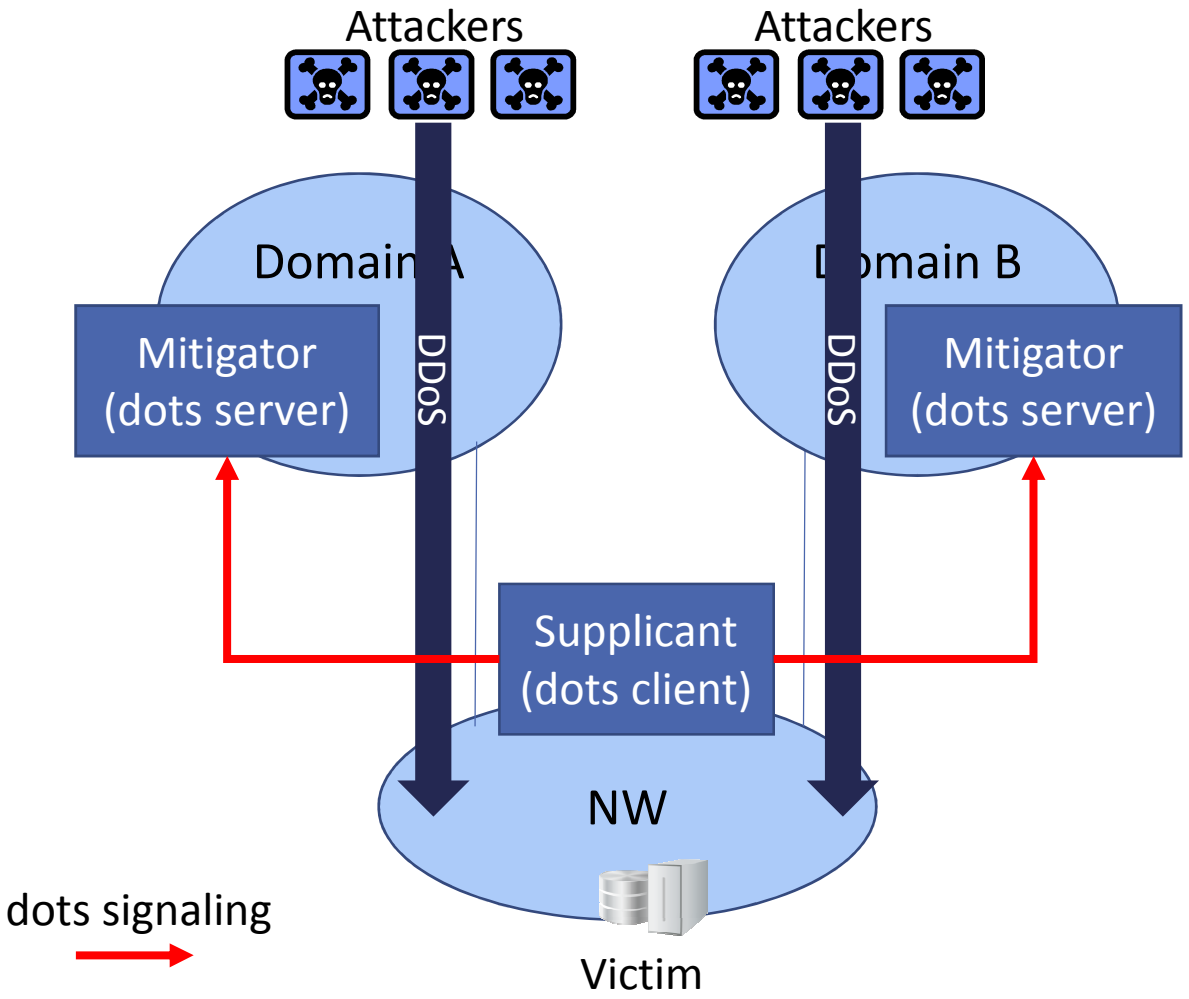
Mandatory information

- IP address of defense target
- Instruction (Start/Stop)
- Authorization information

Optional information

- Traffic volume, type of attack etc,…
  - Can be used for choice of DDoS protection methods
  - Though optional information is useful, let leave the final decision to upper DDoS protection entity.

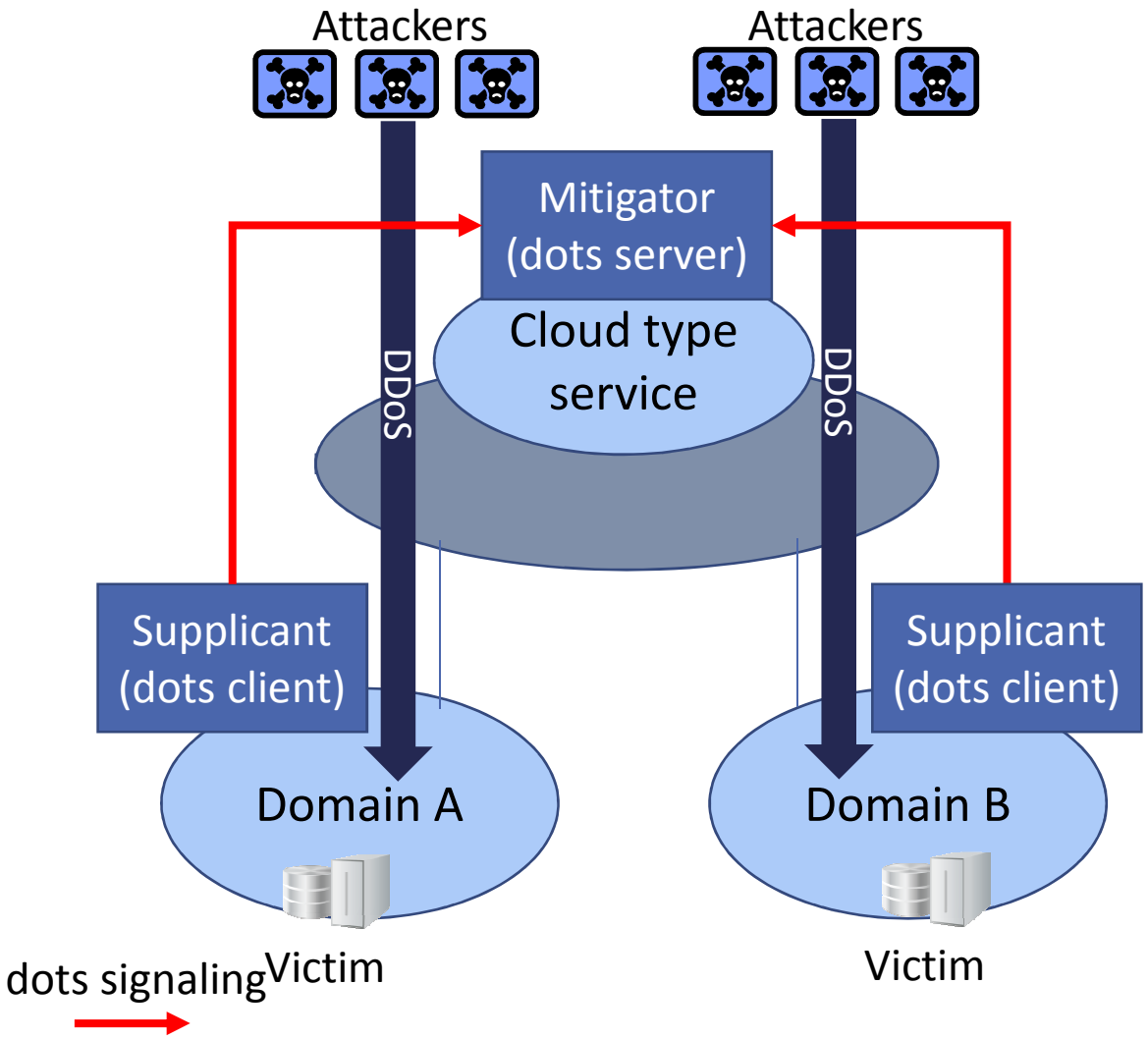
Inter-domain usecase1: Multi-home model



- one supplicant
- multi mitigators

- The common signaling protocol can protect a service in one-stop by protecting both links connected to different domain.

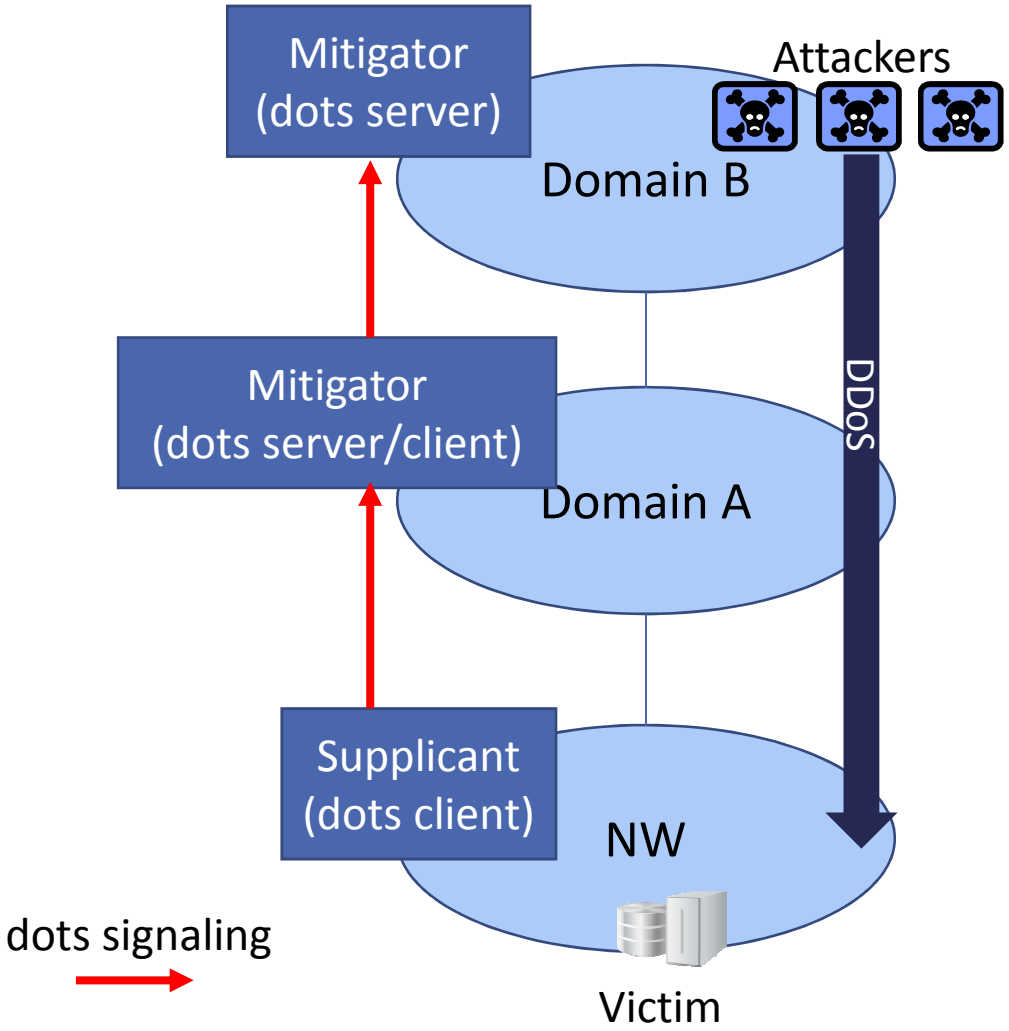
Inter-domain usecase2: Cloud model



- multi supplicants
- one mitigator

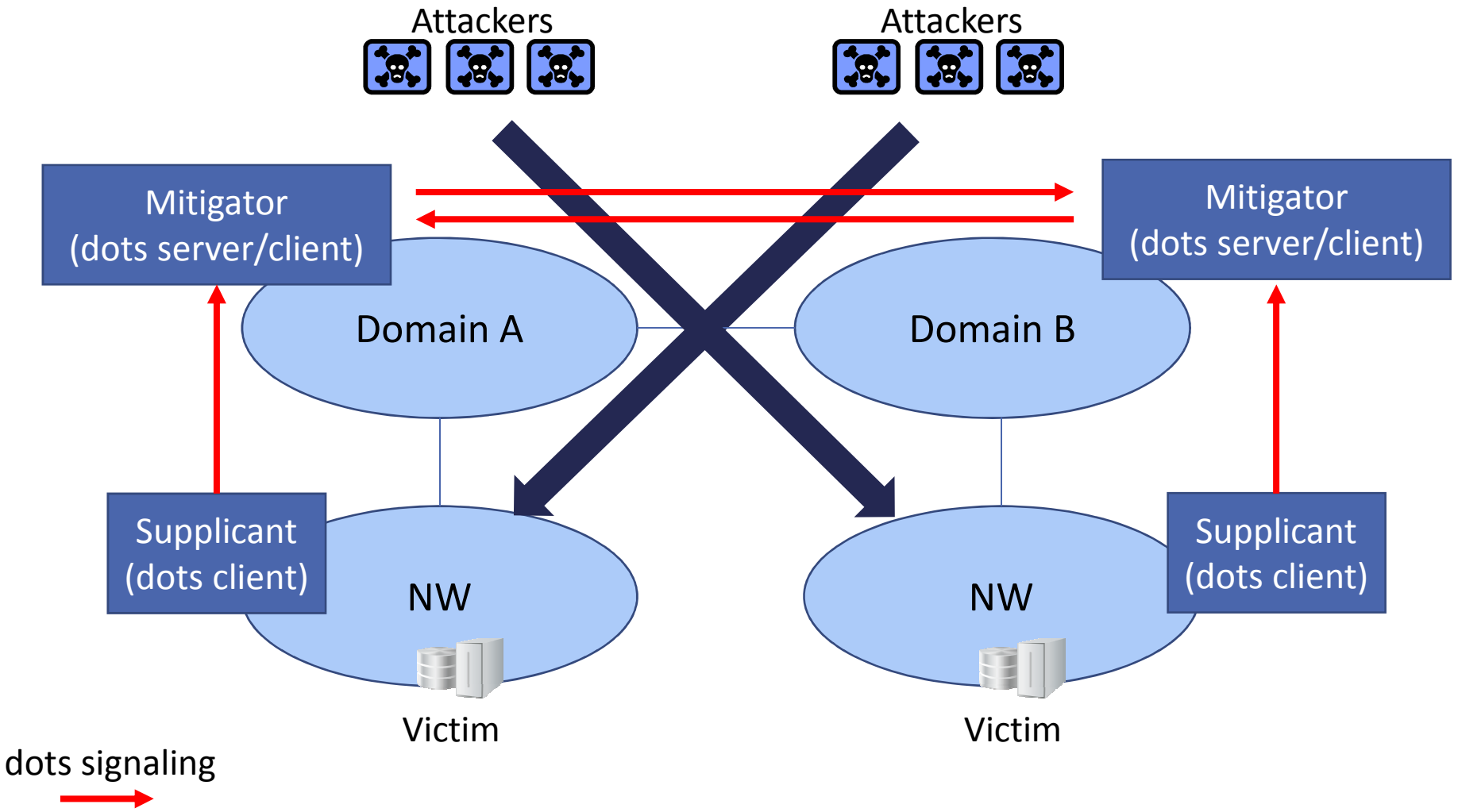
- Cloud type of DDoS mitigation service provides common signaling interface, so any services in different domain can use the mitigator.

Inter-domain usecase3: Delegation model



- a mitigator can be supplicant and vice versa.
- The mitigator in a domain can delegate the burden of protection to other domains by dots signaling.

Cooperative DDoS Mitigation with DOTS Signaling



Nextstep

Improvements

- Align terminology with other drafts.
- Illustrate inter-domain usecase in more detail.

Nextstep

- Can it be merged into one usecase draft?