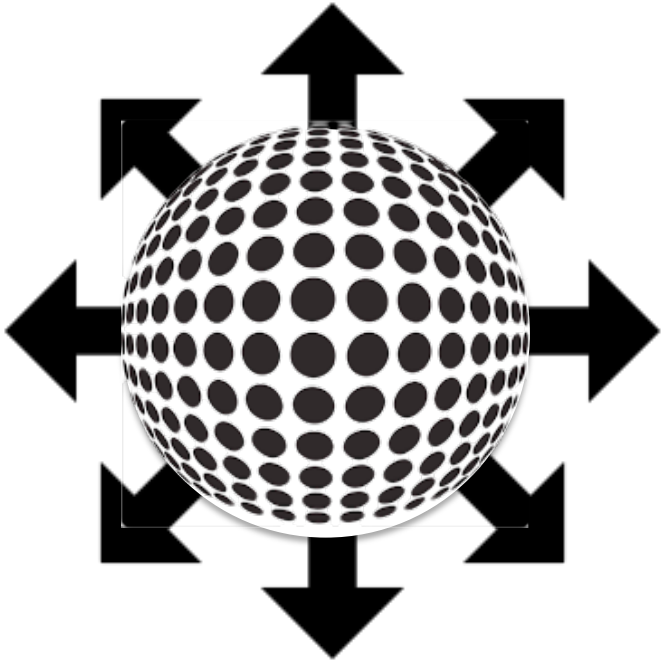


DDoS Open Threat Signaling (DOTS) Working Group

draft-ietf-dots-use-cases-00

Roland Dobbins – Arbor Networks

Stefan Fouant – Corero Network Security

Daniel Migault – Ericsson

Robert Moskowitz – HTT Consulting

Nik Teague – Verisign

Liang 'Frank' Xia – Huawei

Introduction & Context

draft-ietf-dots-use-cases-00 Summary

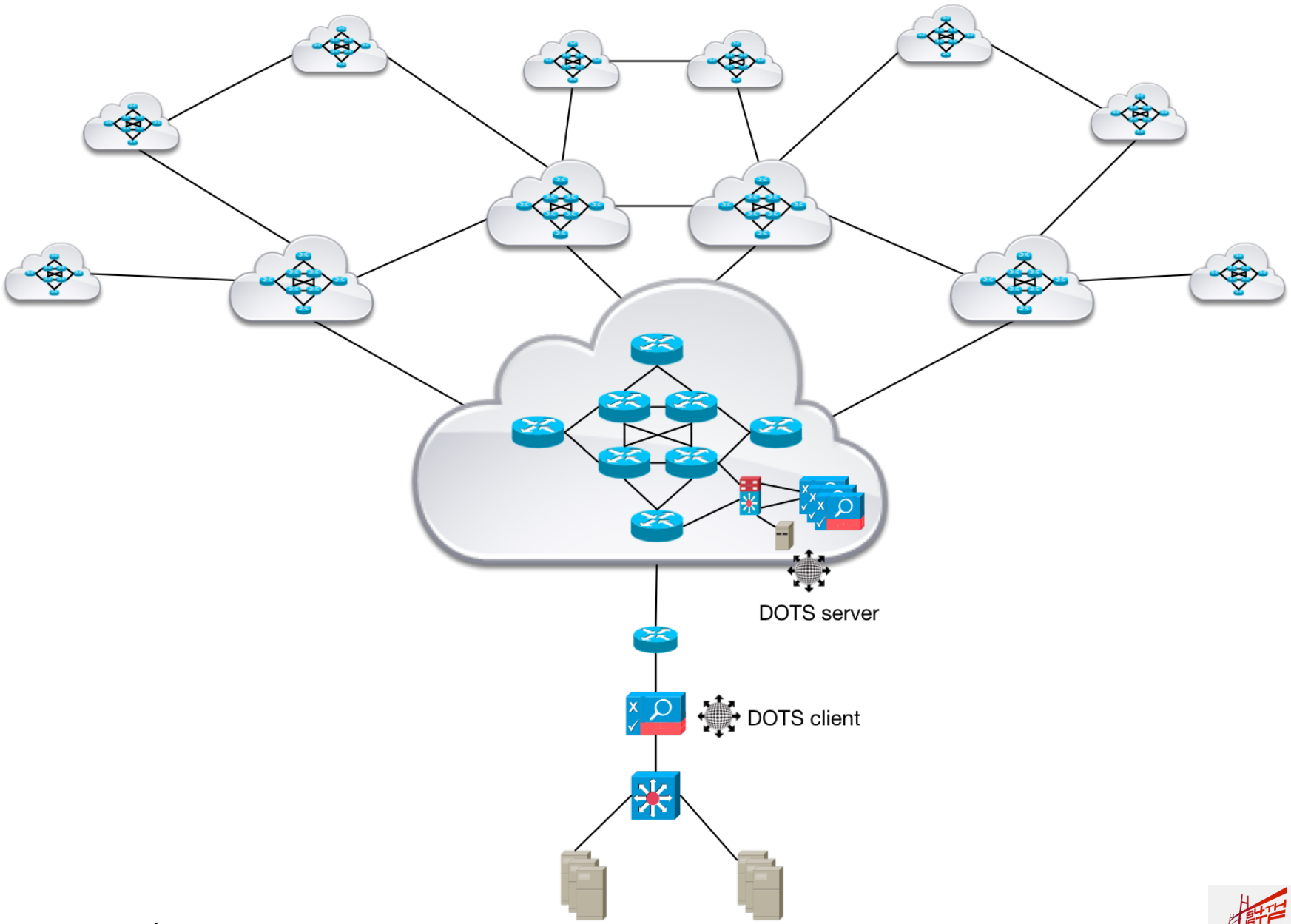
- Provides example use-cases for DOTS (actually, categories).
- All examples can be CE/PE or PE/PE.
- Room for wide variation within each category (see 4.1.1).
- All DOTS communications in each example can be directly between DOTS servers and DOTS clients, or mediated by DOTS relays.
- DOTS relays can forward messages between DOTS clients and servers using either stateless transport, stateful transport, or a combination of the two.
- DOTS relays can aggregate service requests, status messages, and responses.
- DOTS relays can filter service requests, status messages, and responses

draft-ietf-dots-use-cases-00 Summary (cont.)

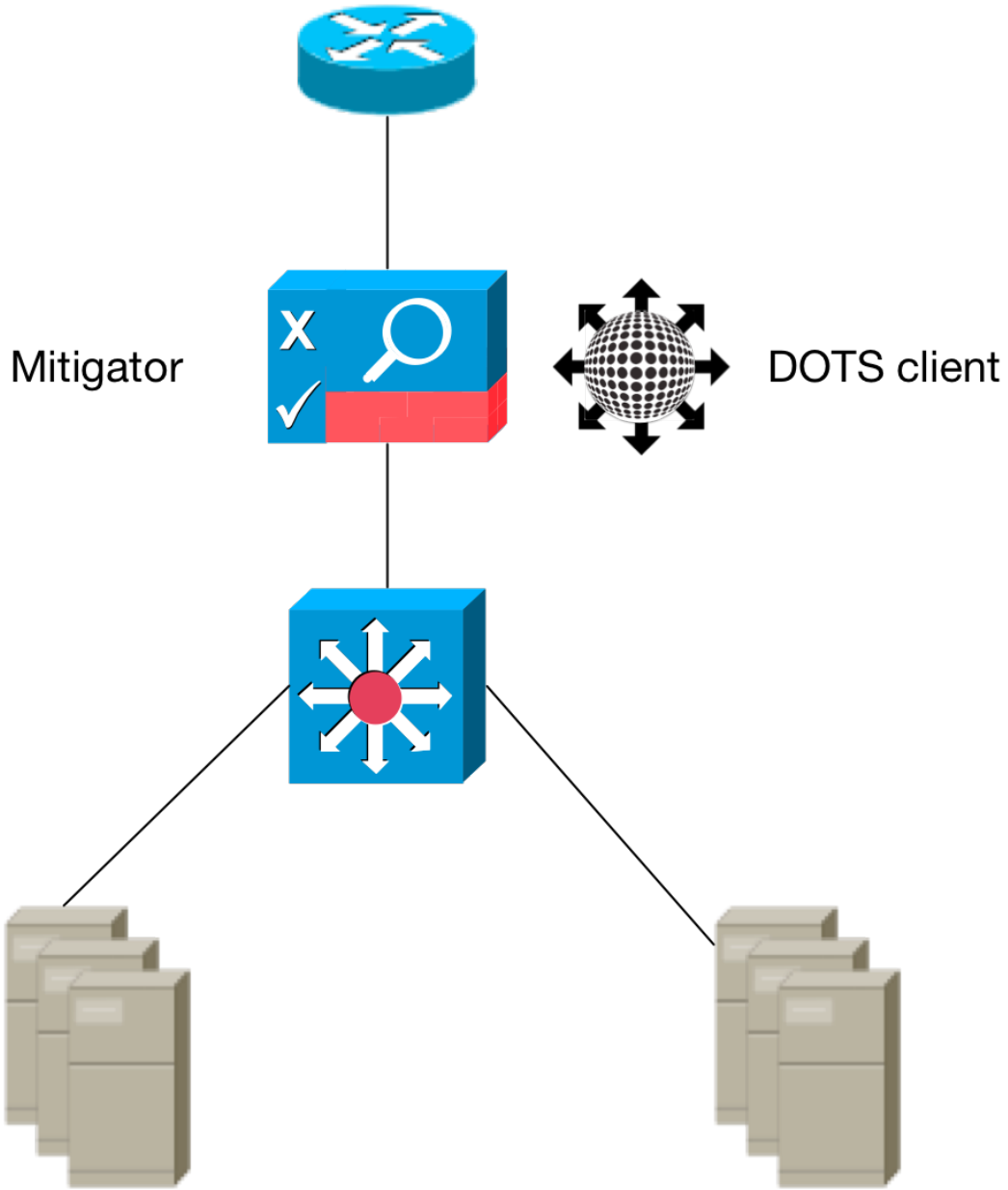
- Use-cases in -00 are not exhaustive, are illustrative.
- Use-cases in -00 focus on DDoS mitigation using dedicated mitigation devices. S/RTBH, flowspec, OpenFlow, etc. can also be used to leverage network infrastructure for DDoS mitigation.
- 4.1.1 use-case in this presentation illustrates full DOTS communications cycle, variants.
- Other use-cases in this presentation are summarized ‘diffs’ illustrating DOTS communications model in widely varying circumstances.
- Use-cases in this presentation focus on protecting servers under DDoS attack on destination networks. DOTS can also be used to suppress attack traffic on origin networks or as it traverses intermediary networks.

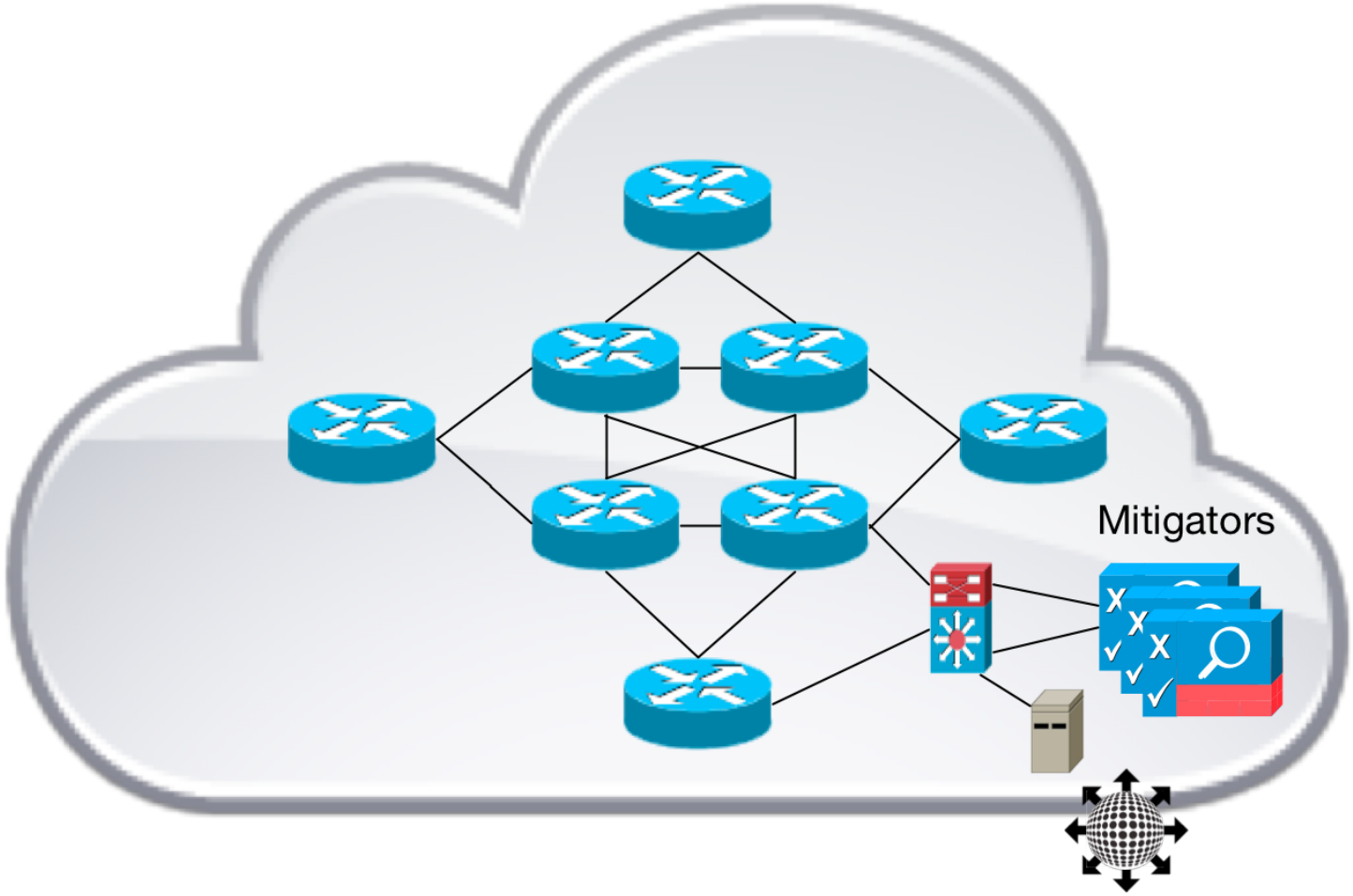
4.1 - Primary Use Cases

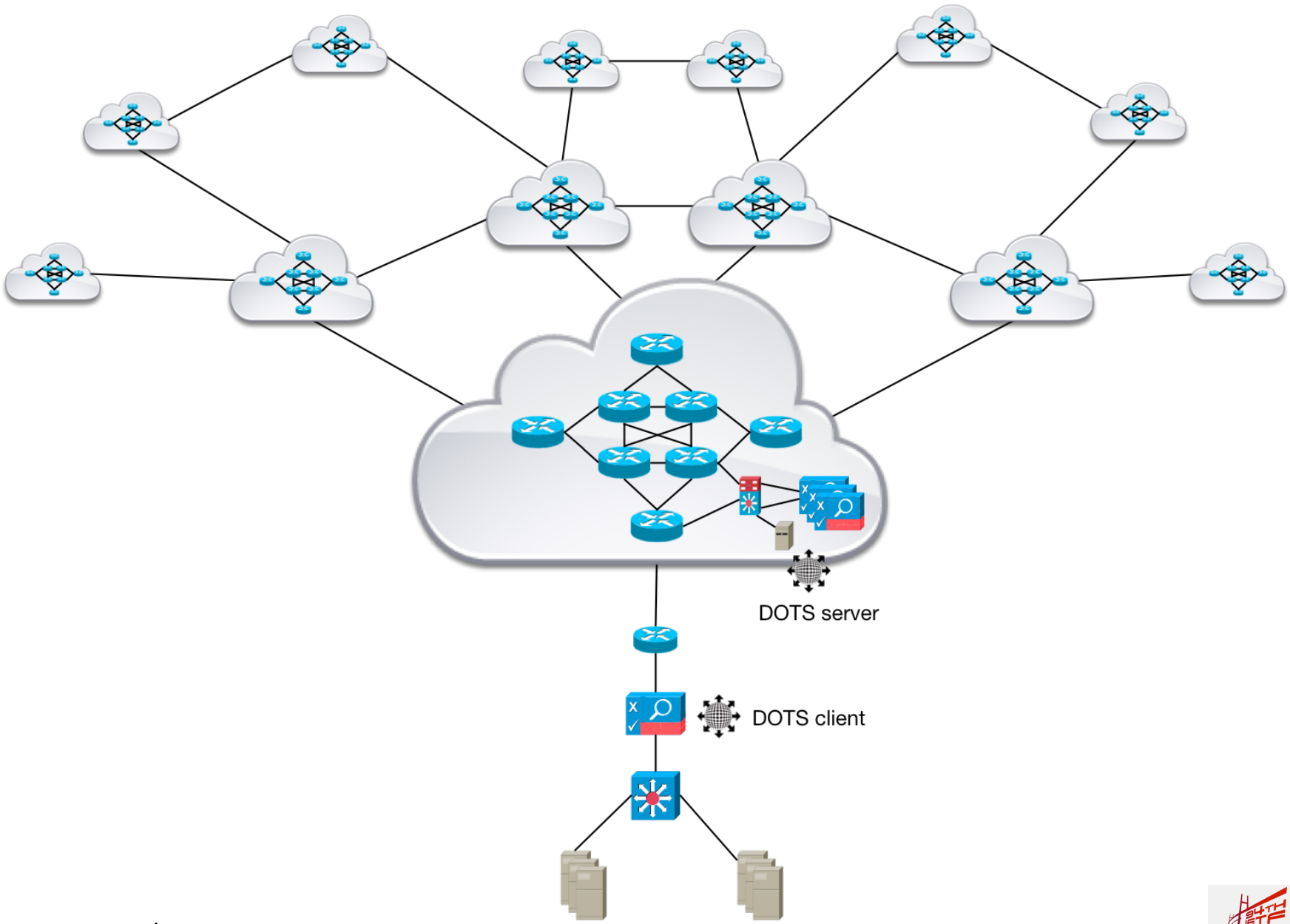
4.1.1 – CPE or PE Mitigators Request Upstream DDoS Mitigation

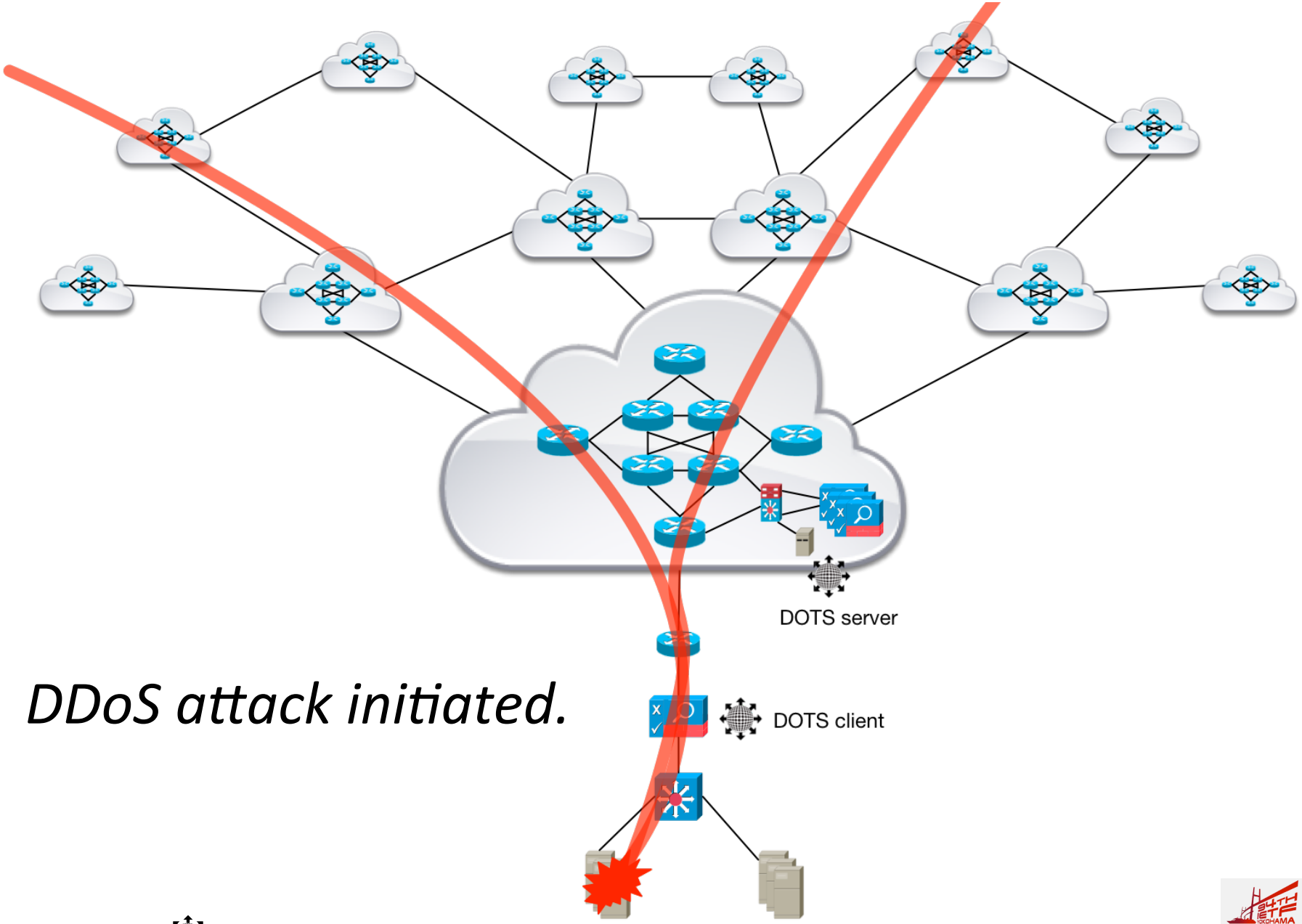


DOTS WG

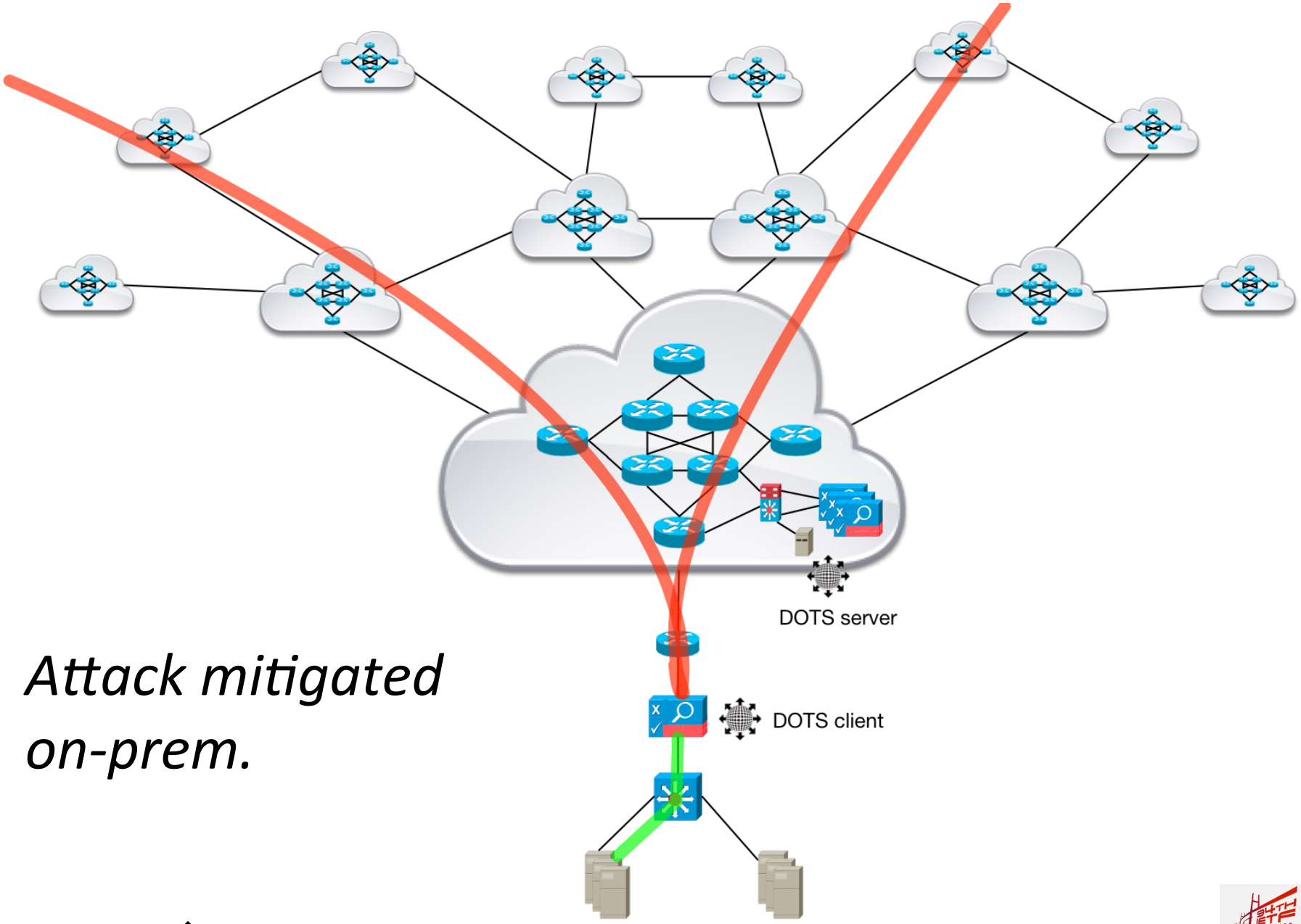

Mitigator
DOTS client


Mitigators
DOTS server

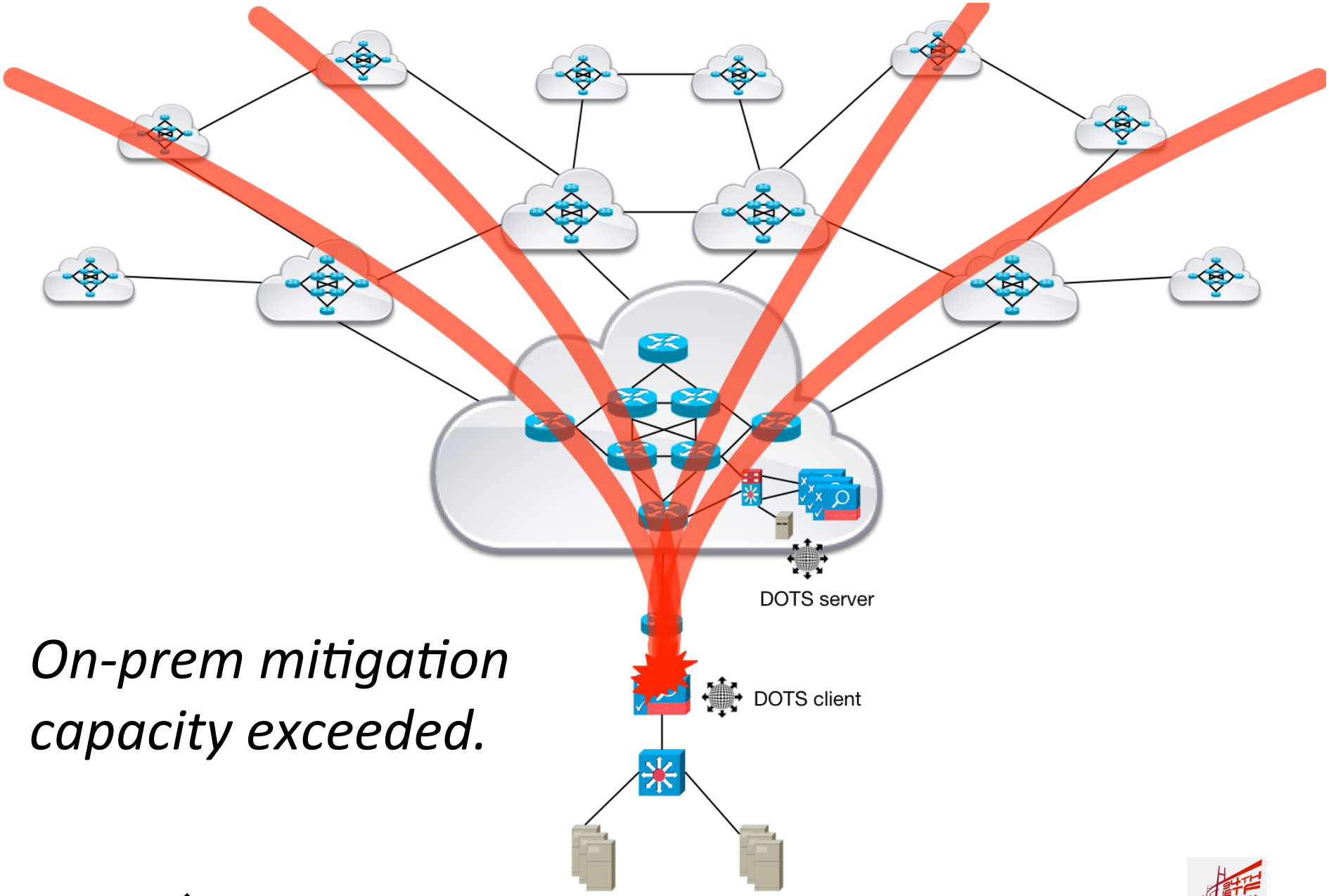

DOTS server
DOTS client



DDoS attack initiated.

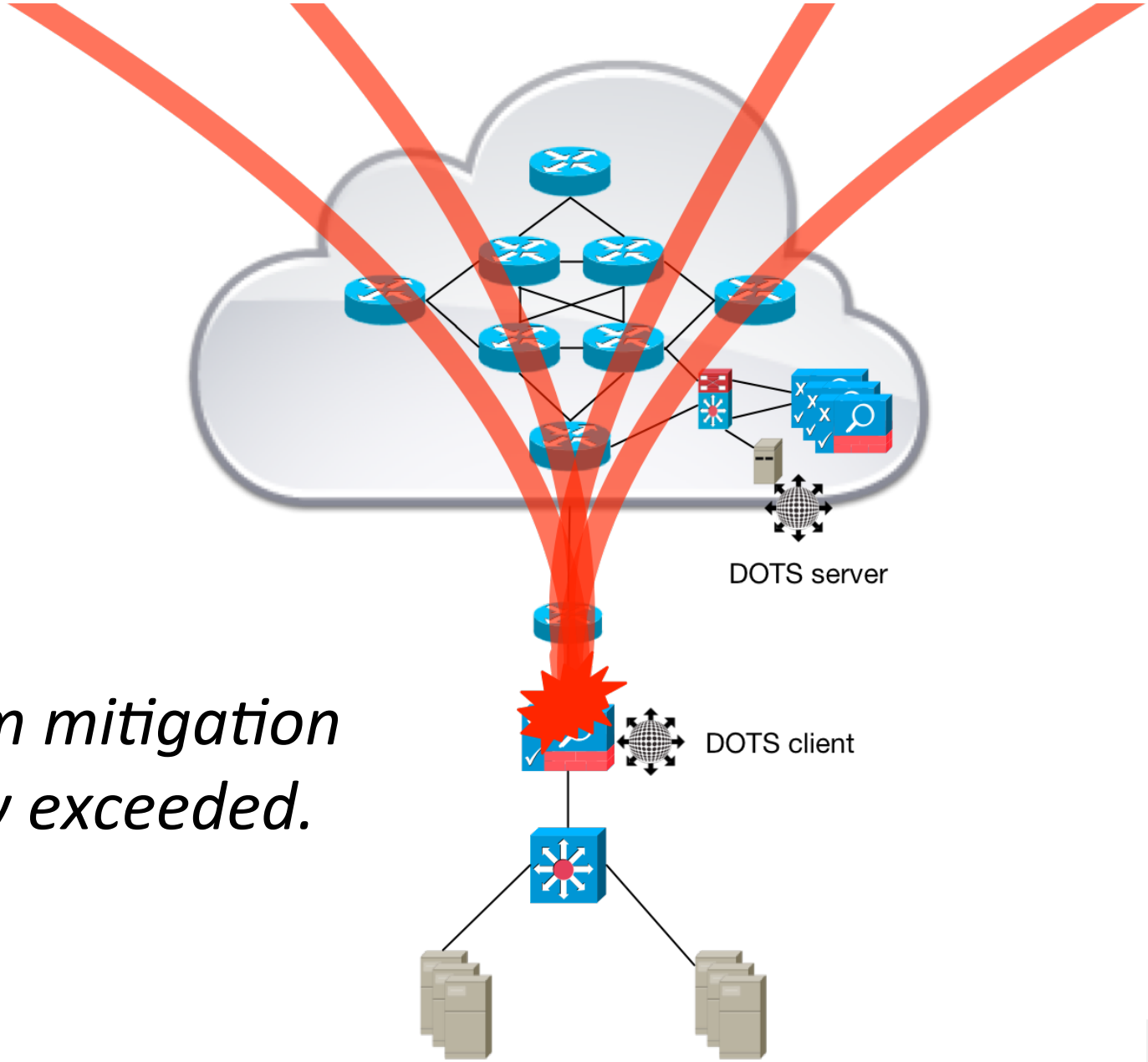


Attack mitigated on-prem.

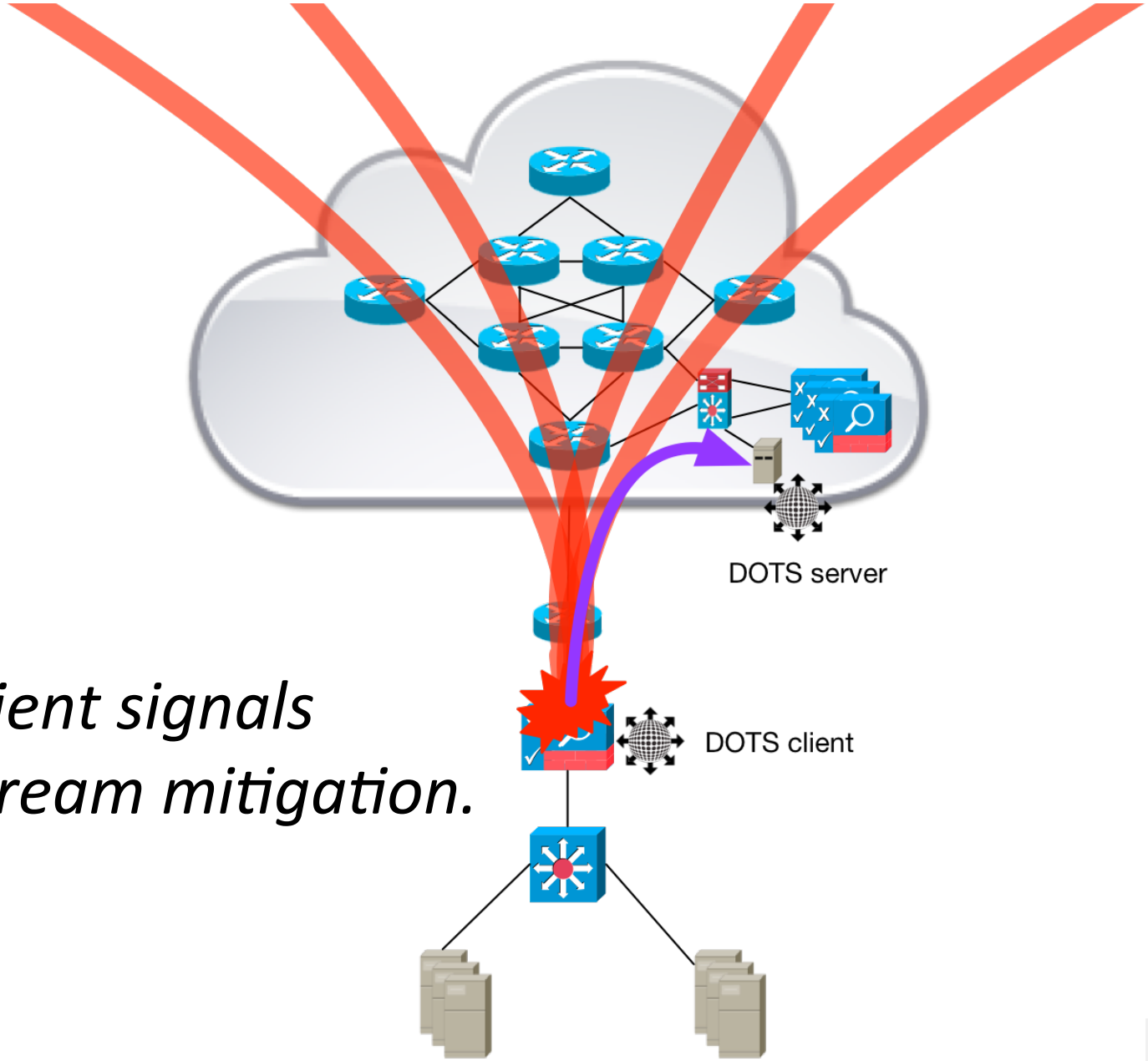


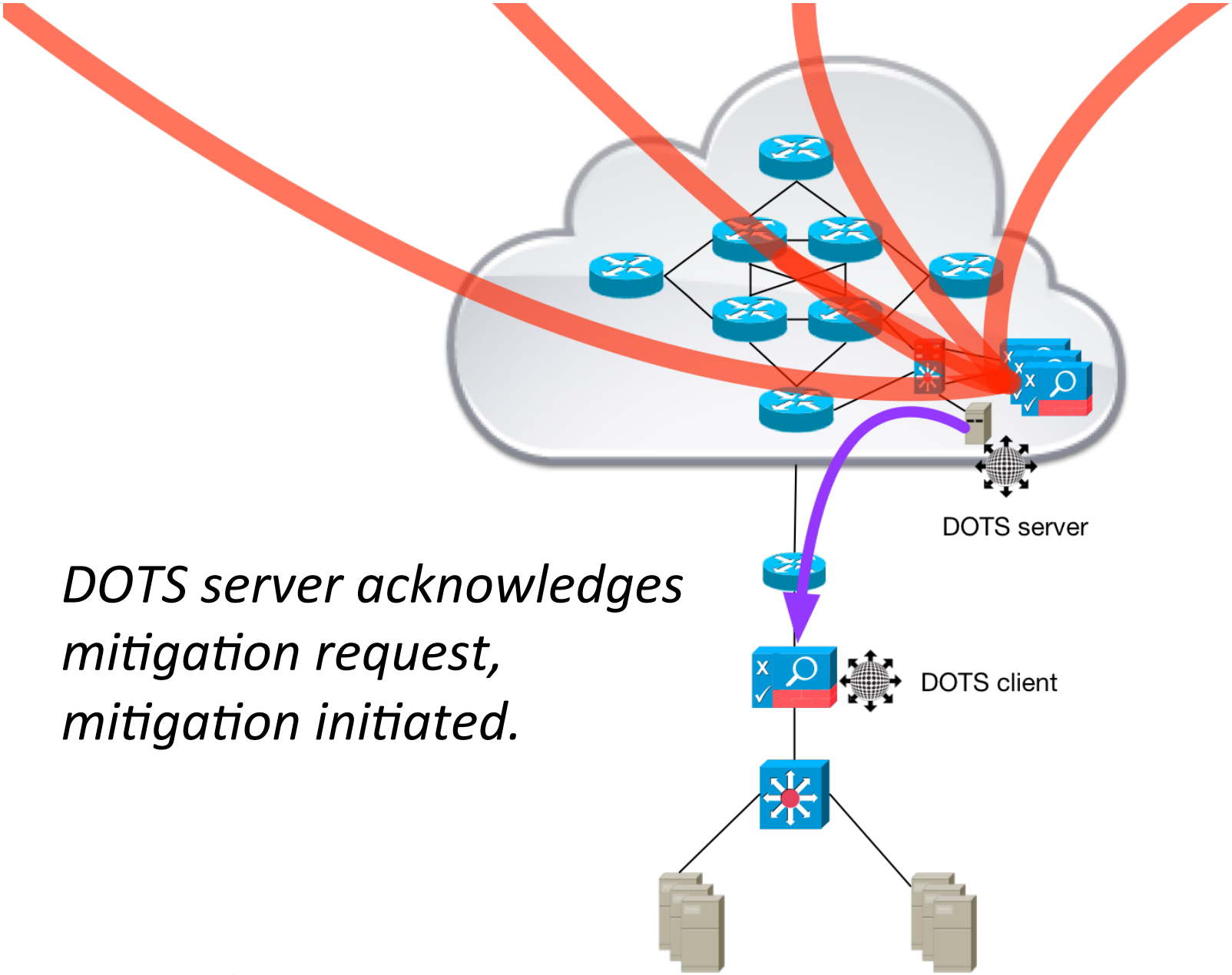
On-prem mitigation capacity exceeded.

On-prem mitigation capacity exceeded.

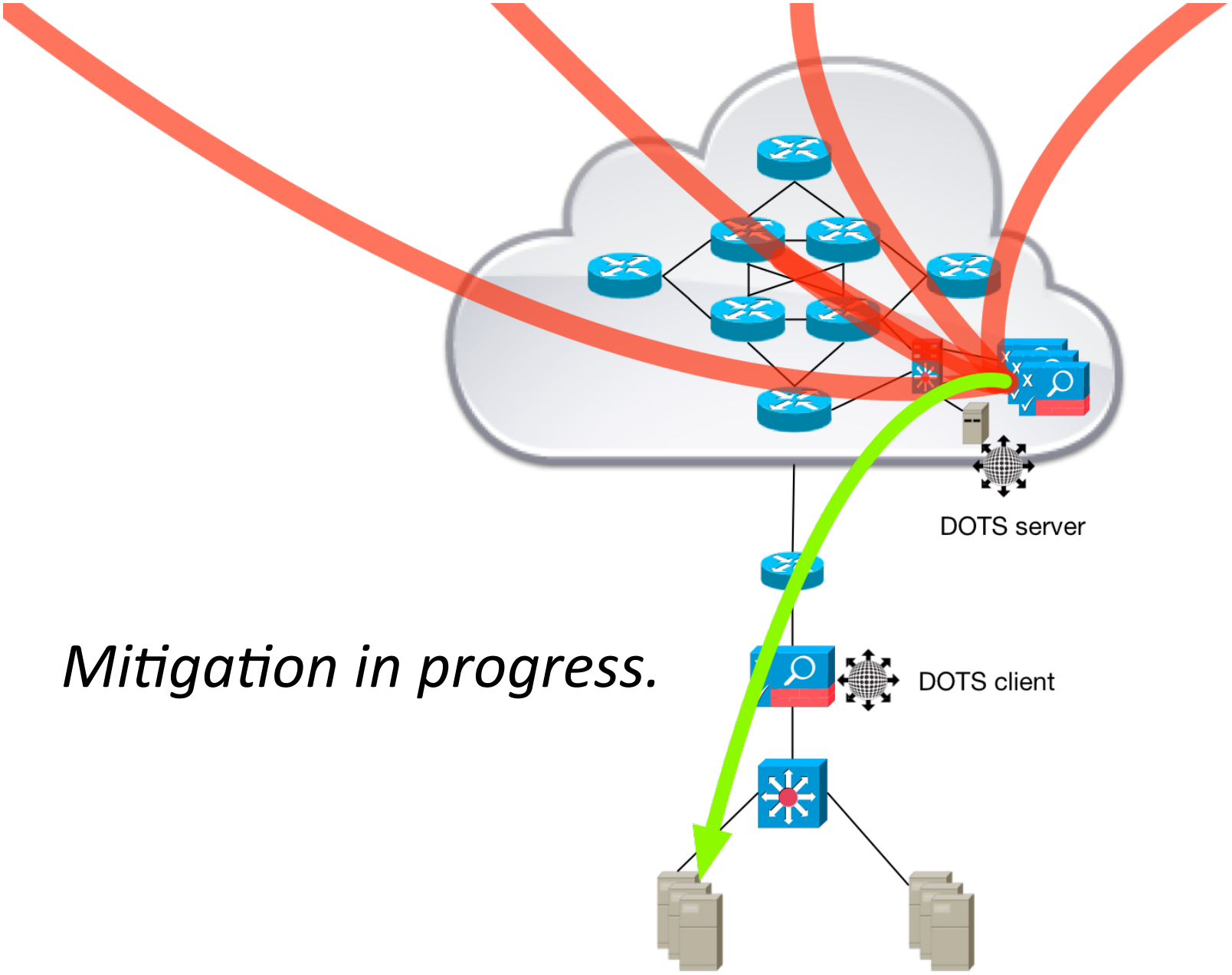


DOTS client signals
for upstream mitigation.



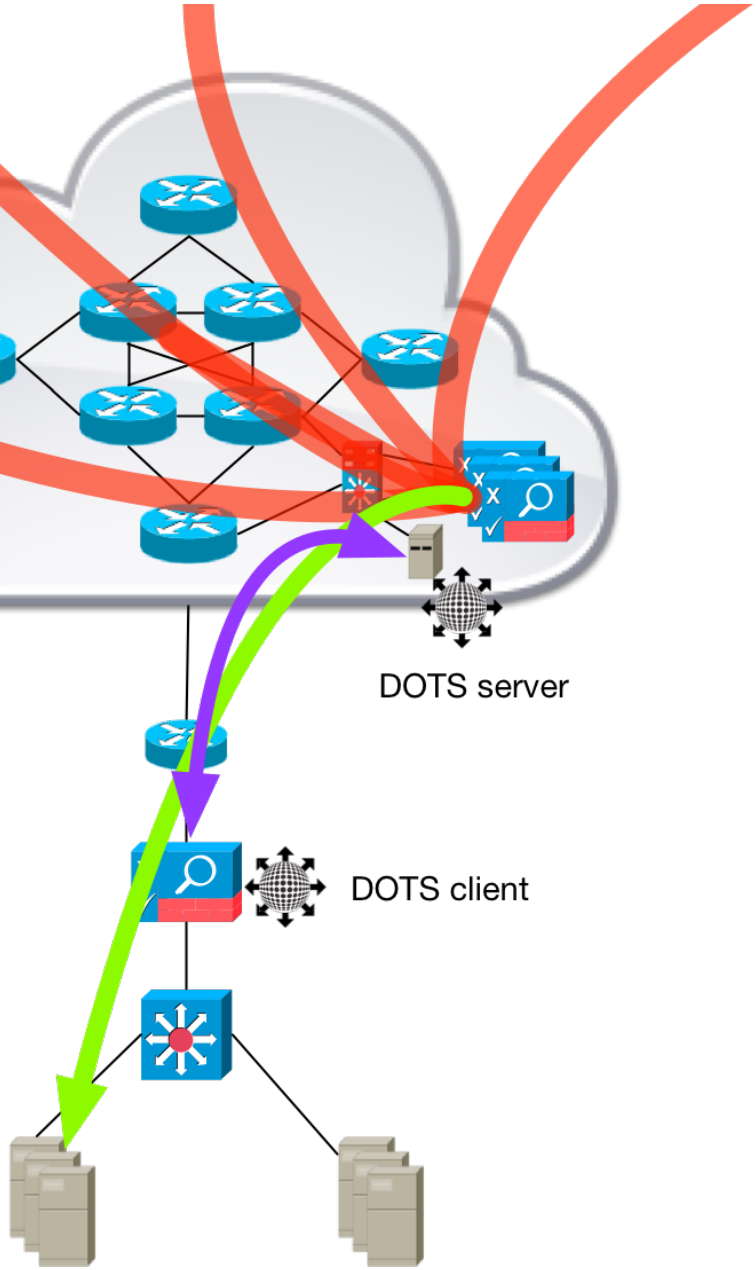


DOTS server acknowledges mitigation request, mitigation initiated.

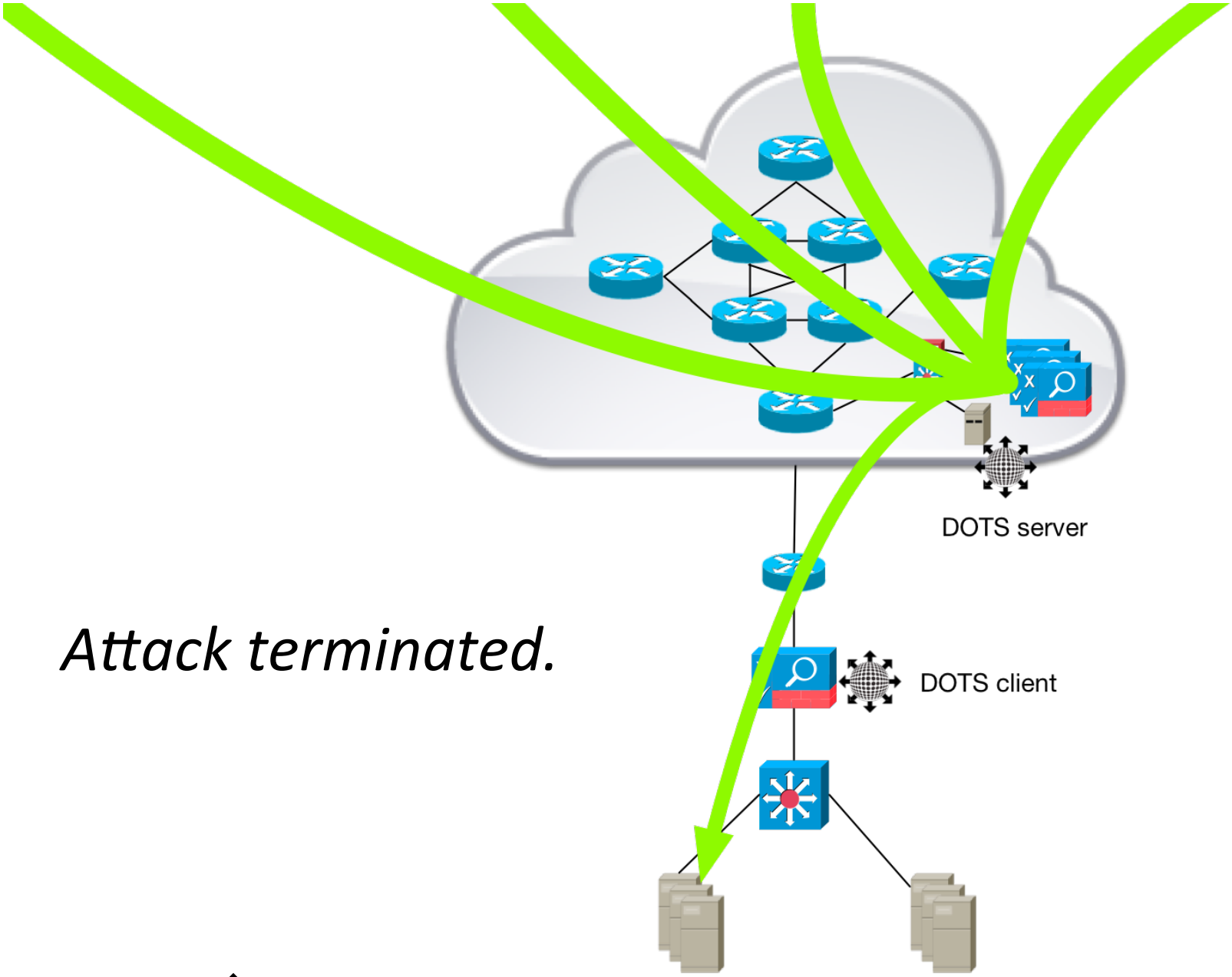


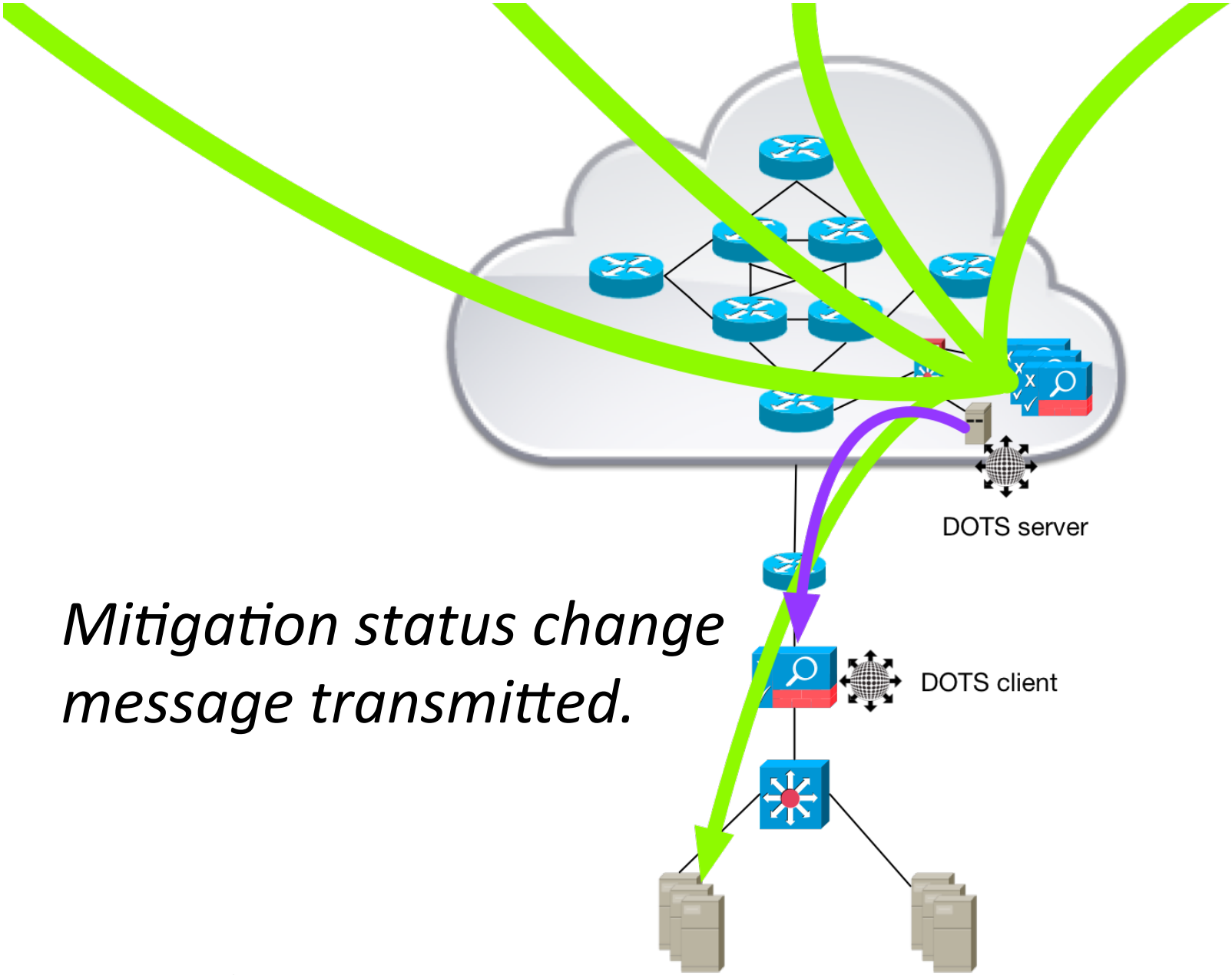
Mitigation in progress.

Status messages exchanged during mitigation – efficacy, mitigation status, etc.

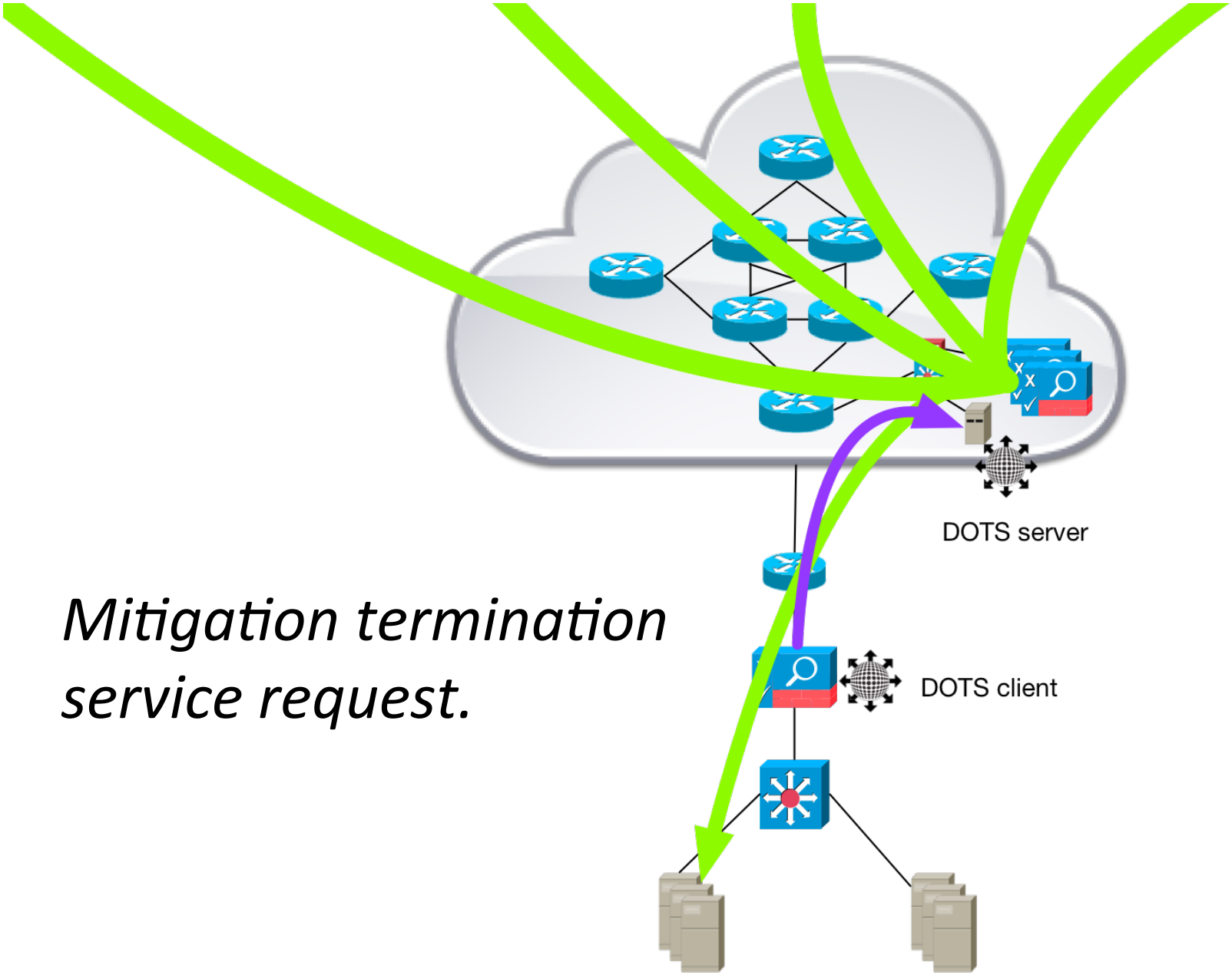


Attack terminated.

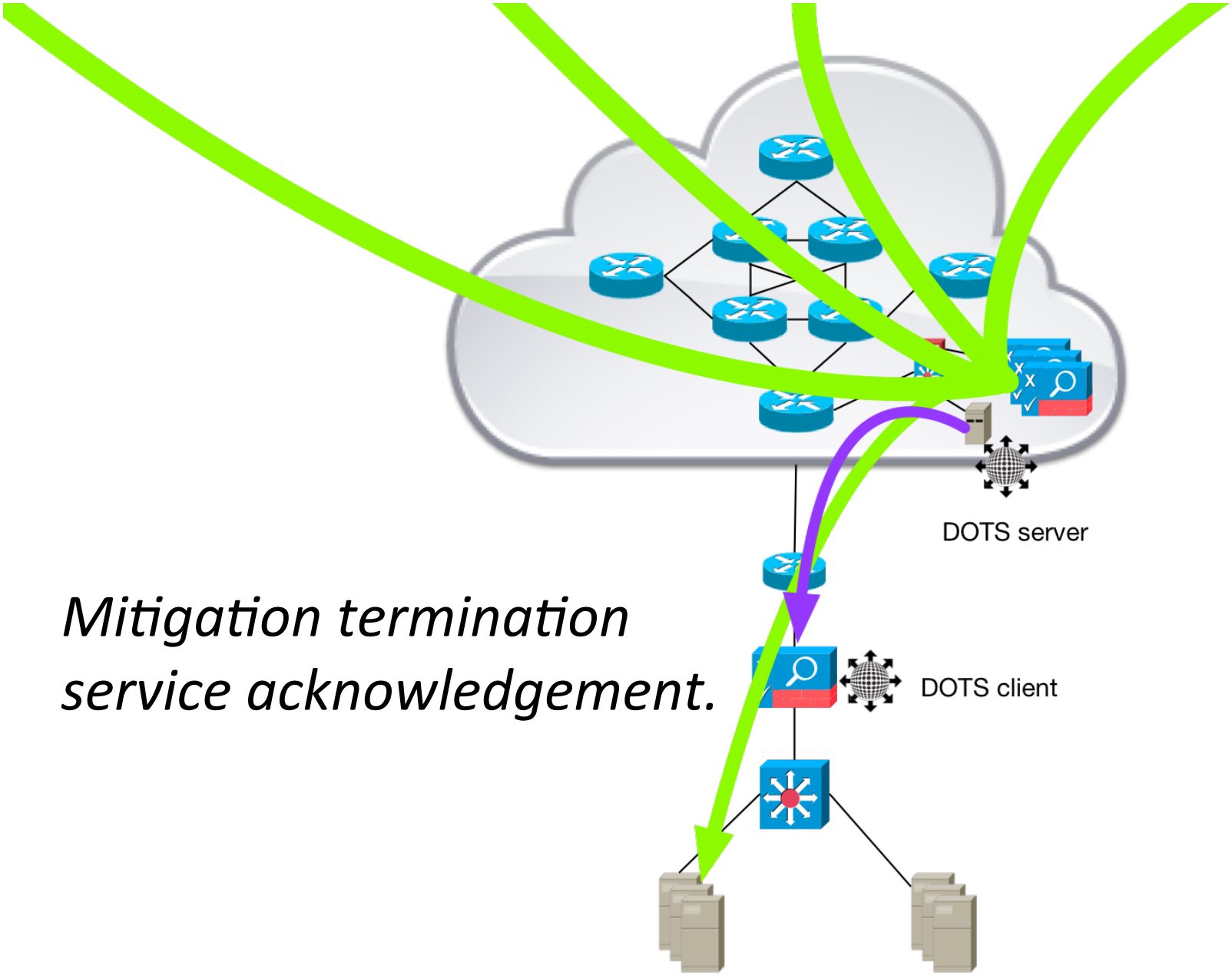




Mitigation status change message transmitted.

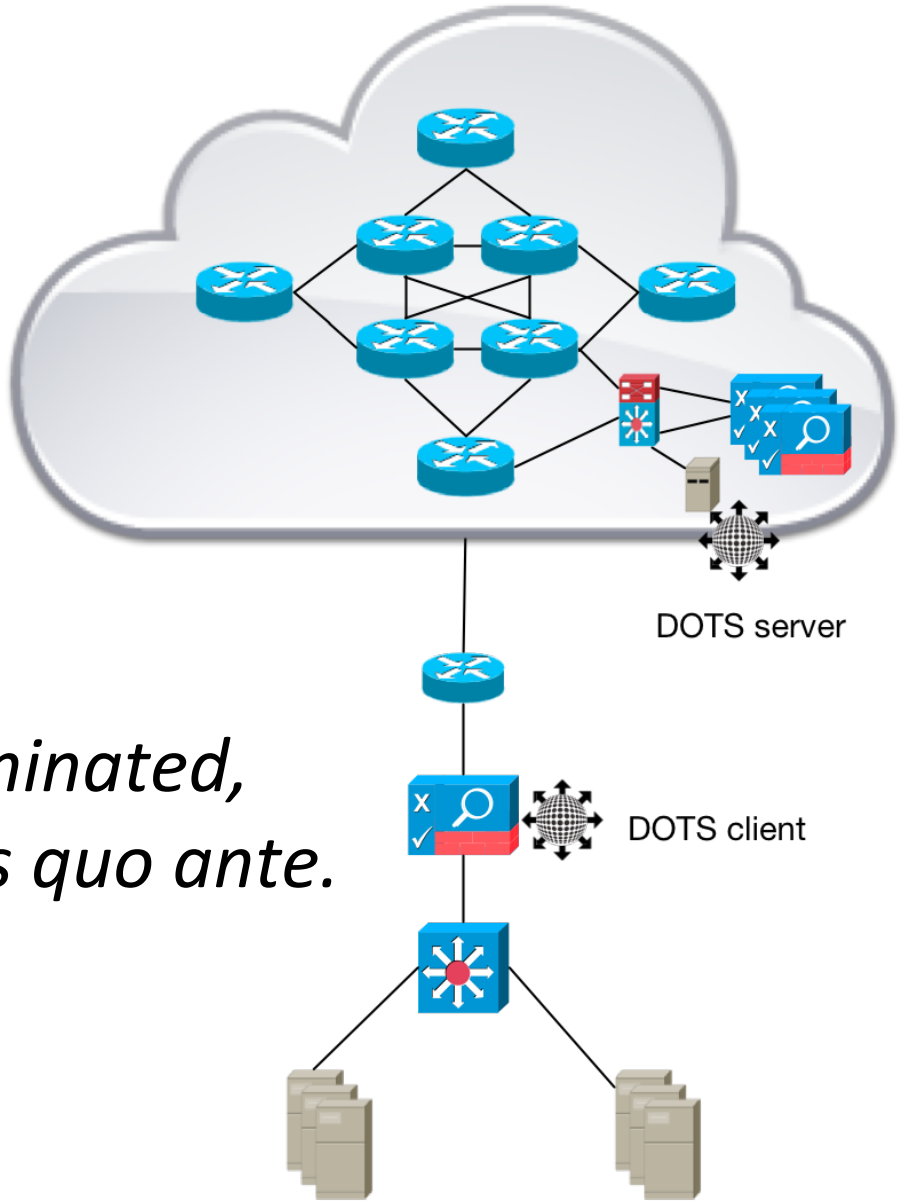


Mitigation termination service request.

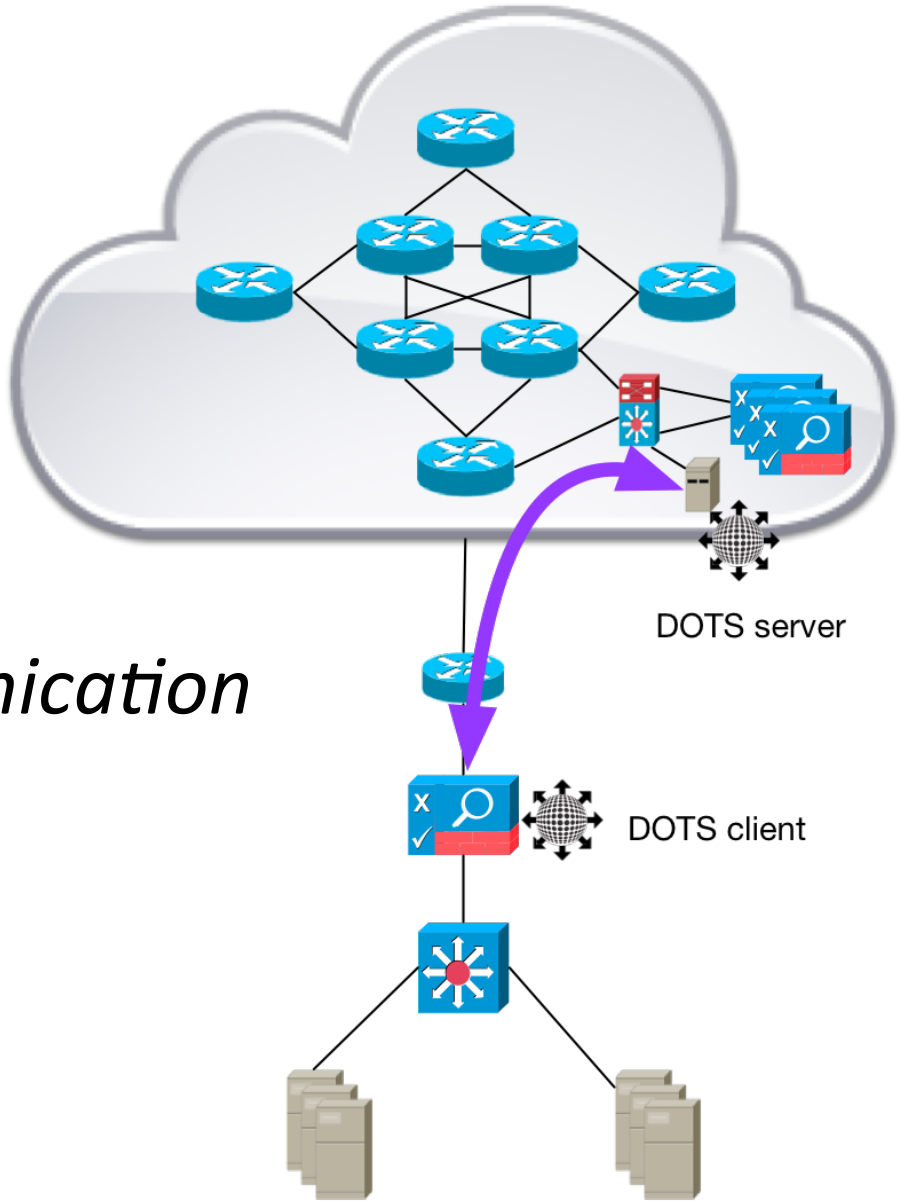


Mitigation termination service acknowledgement.

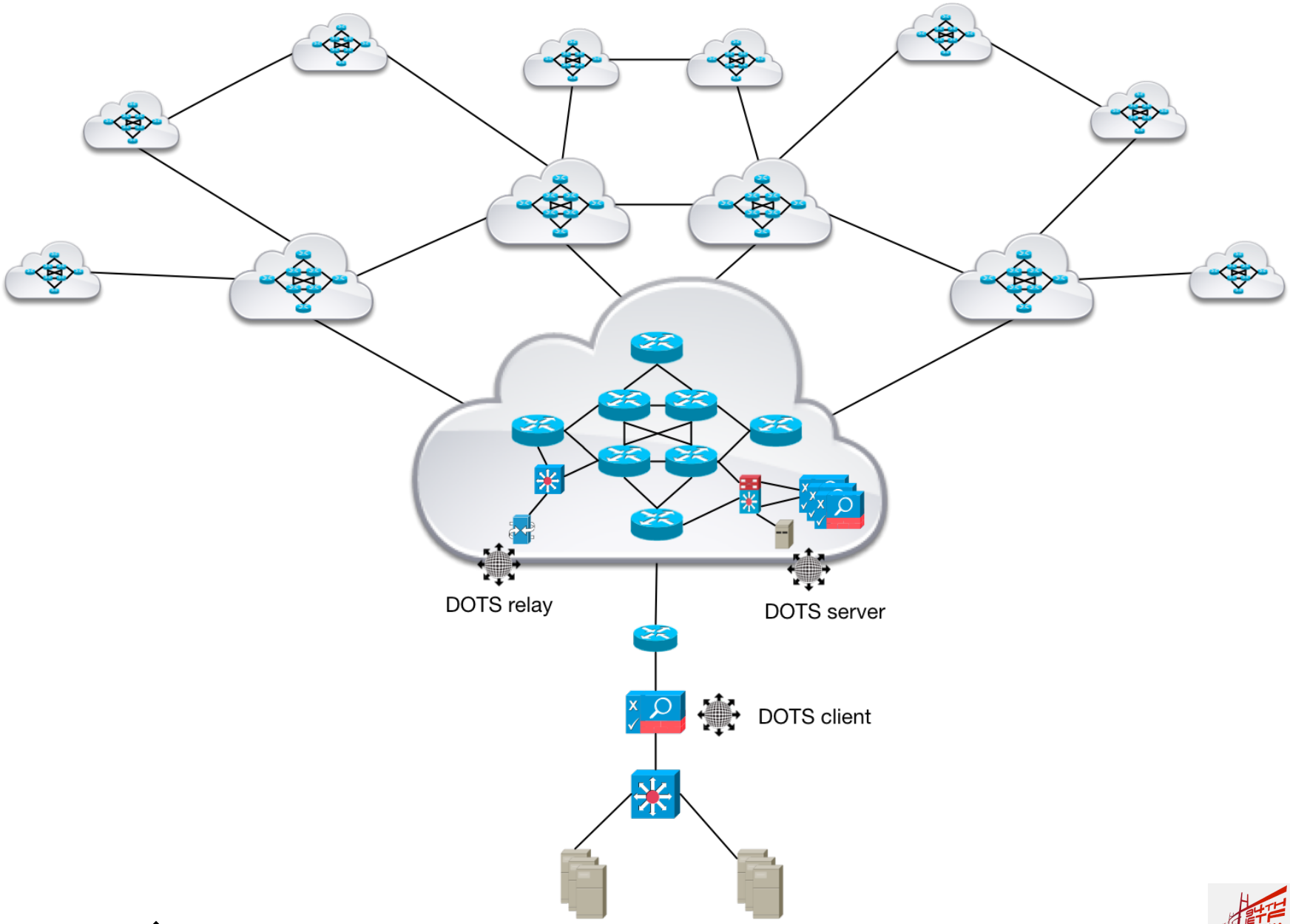
Mitigation terminated, return to status quo ante.

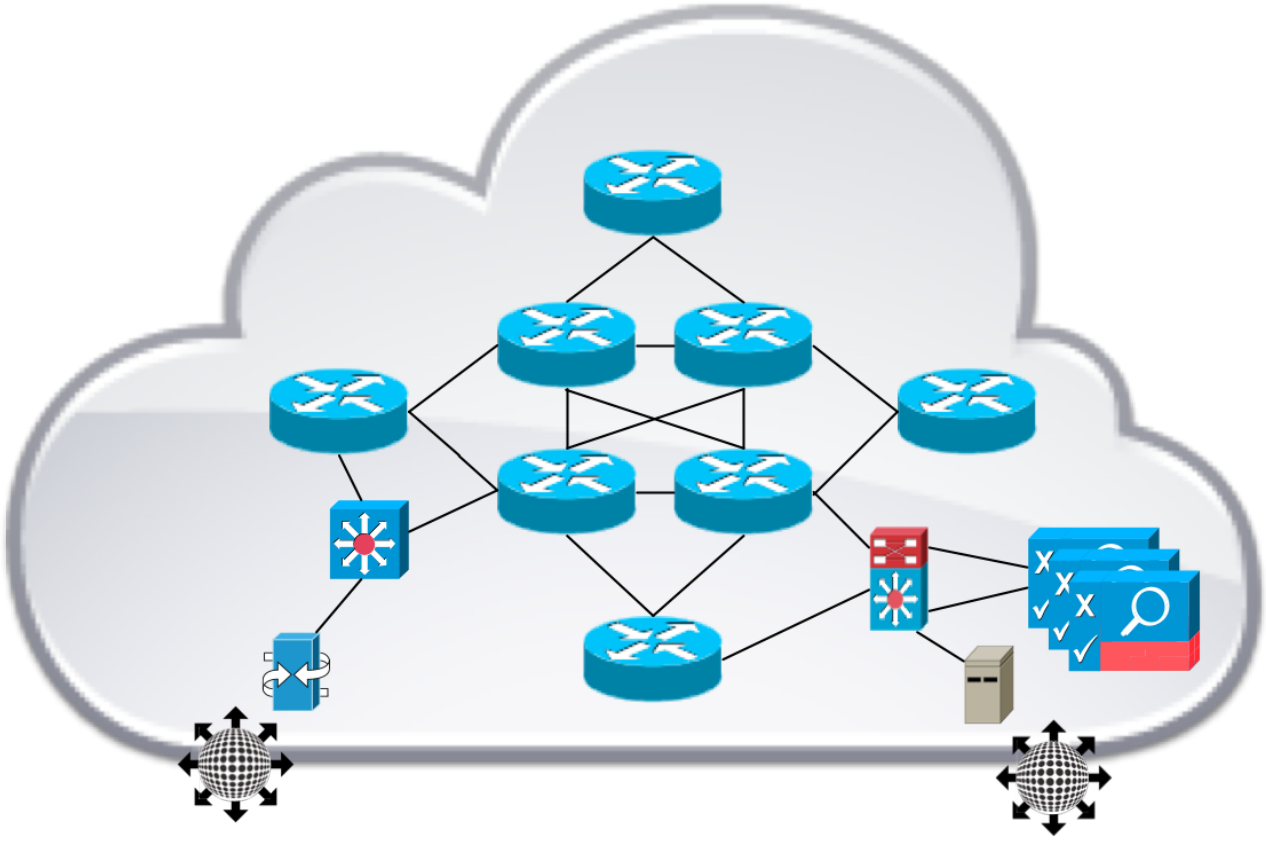


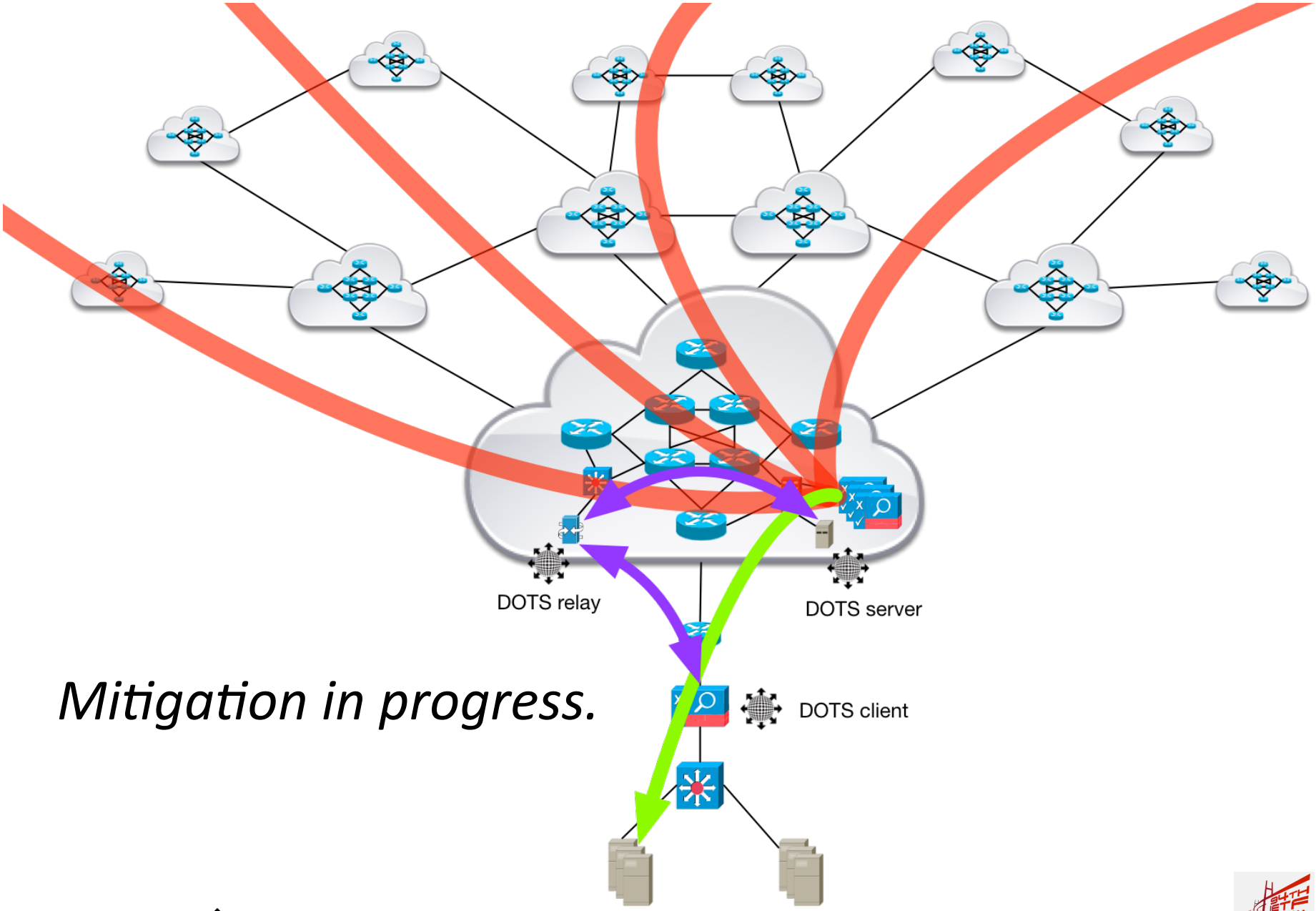
DOTS communication relationships.



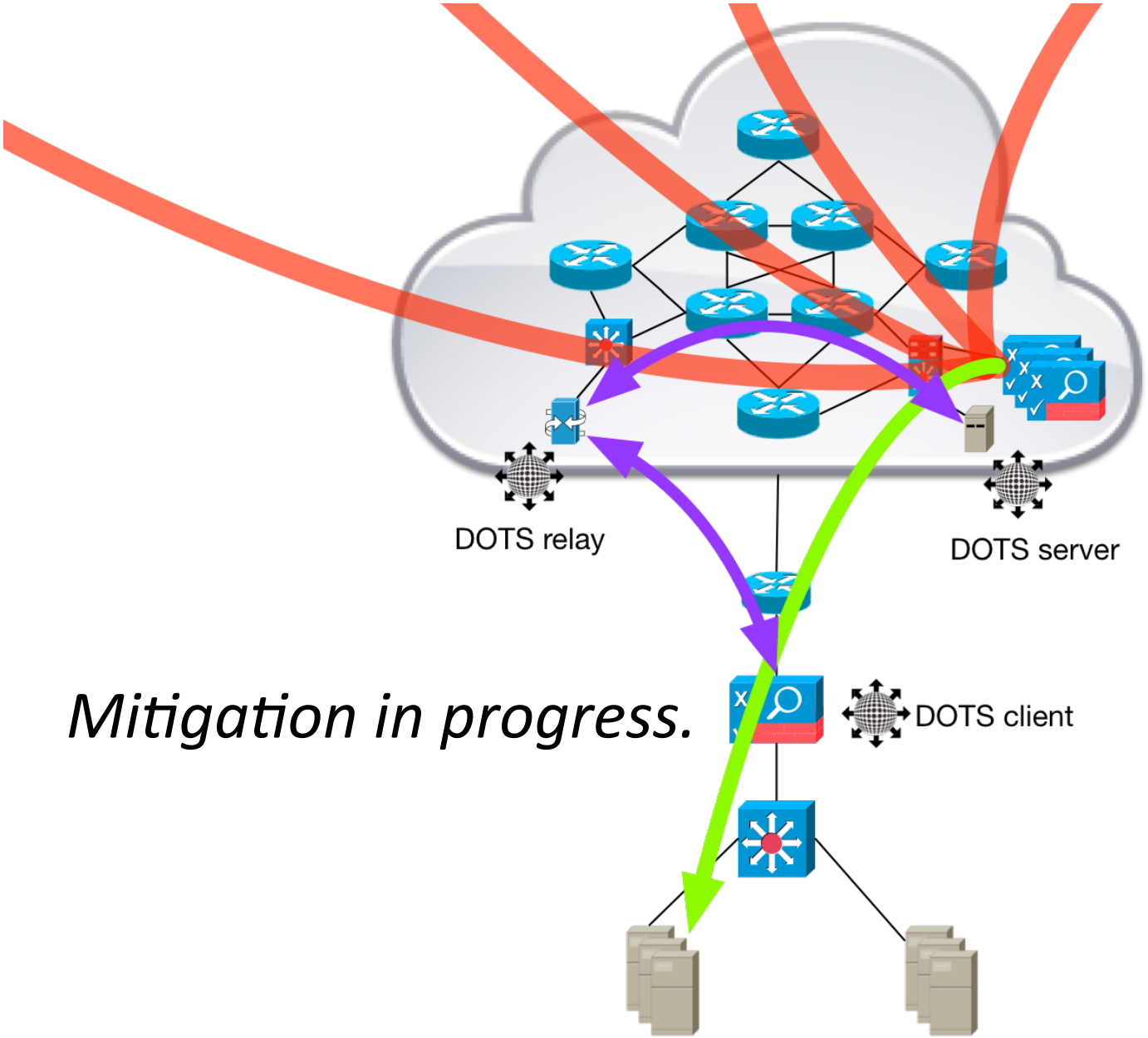
4.1.1 – Variation with DOTS Relay Mediating Communications


DOTS relay
DOTS server
DOTS client

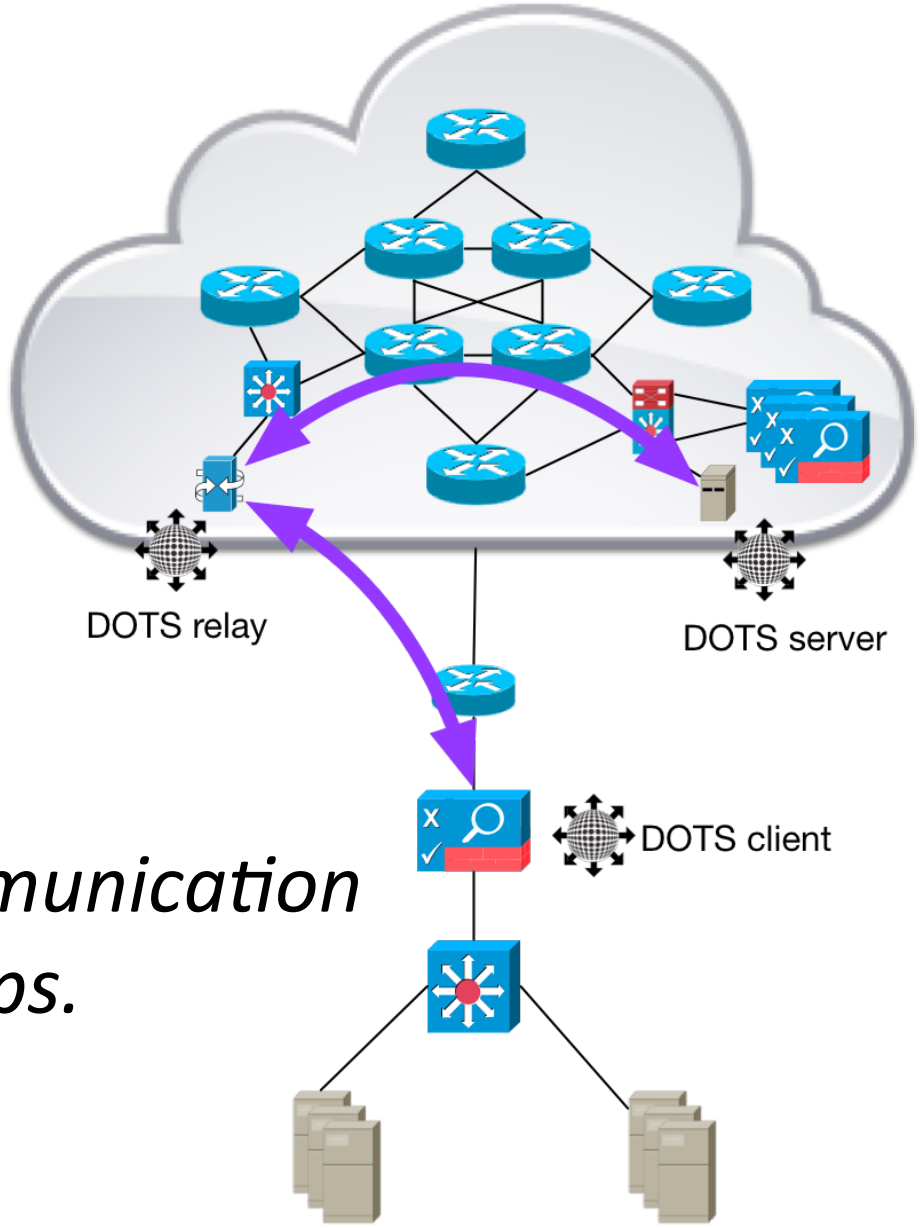

DOTS relay
DOTS server



Mitigation in progress.

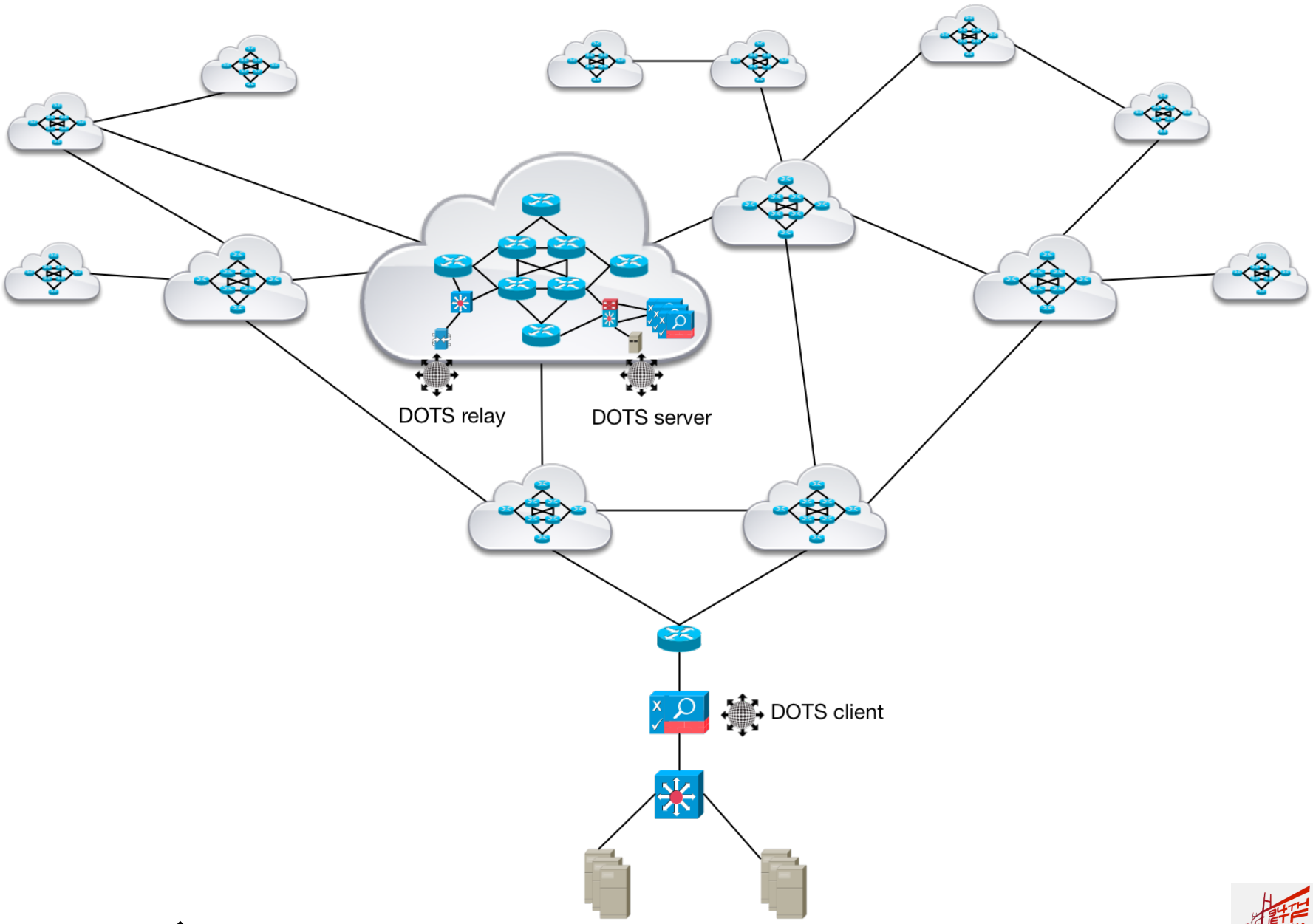


Mitigation in progress.

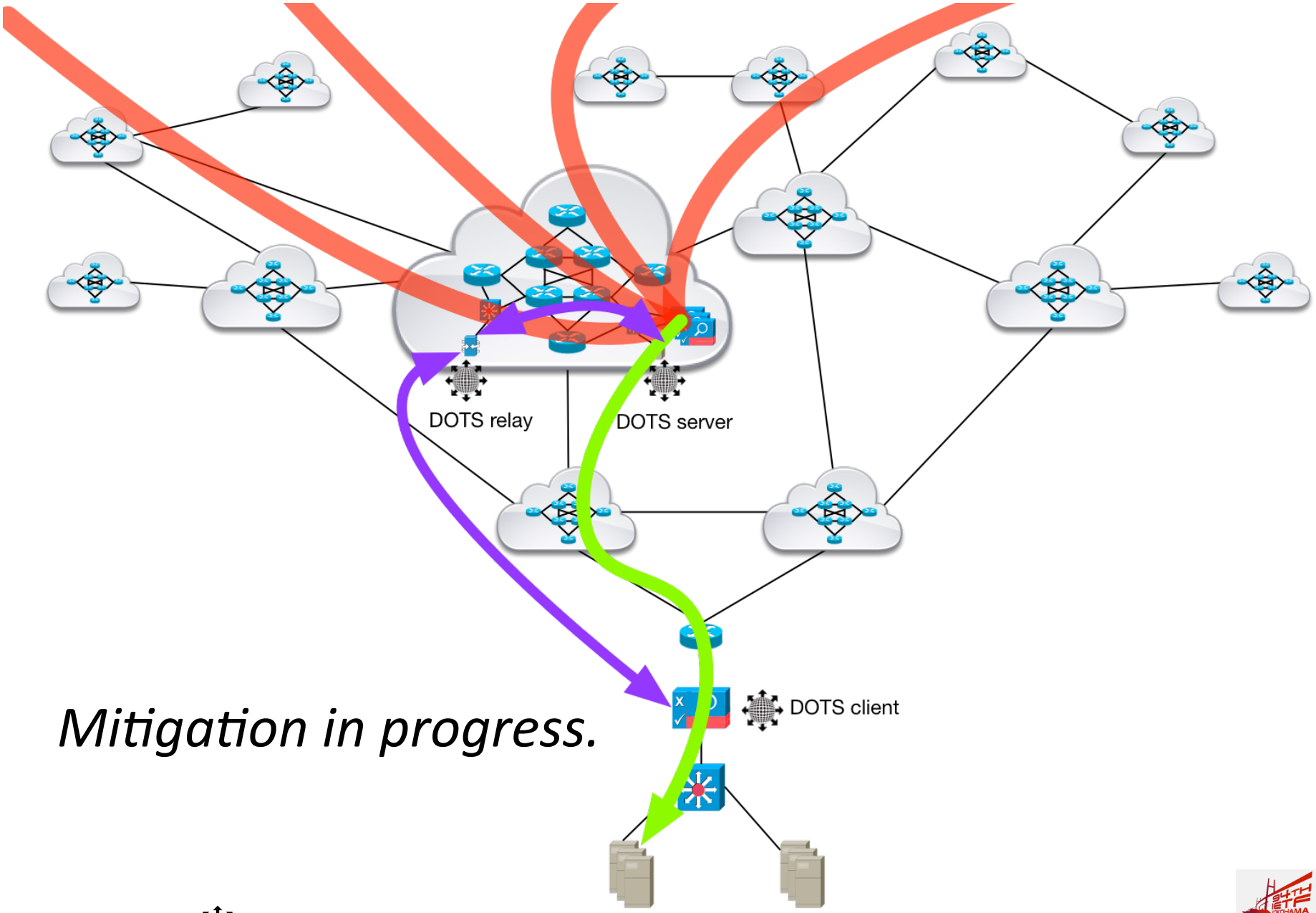


DOTS communication relationships.

4.1.1 – Variation with Overlay DDoS Mitigation Service Provider

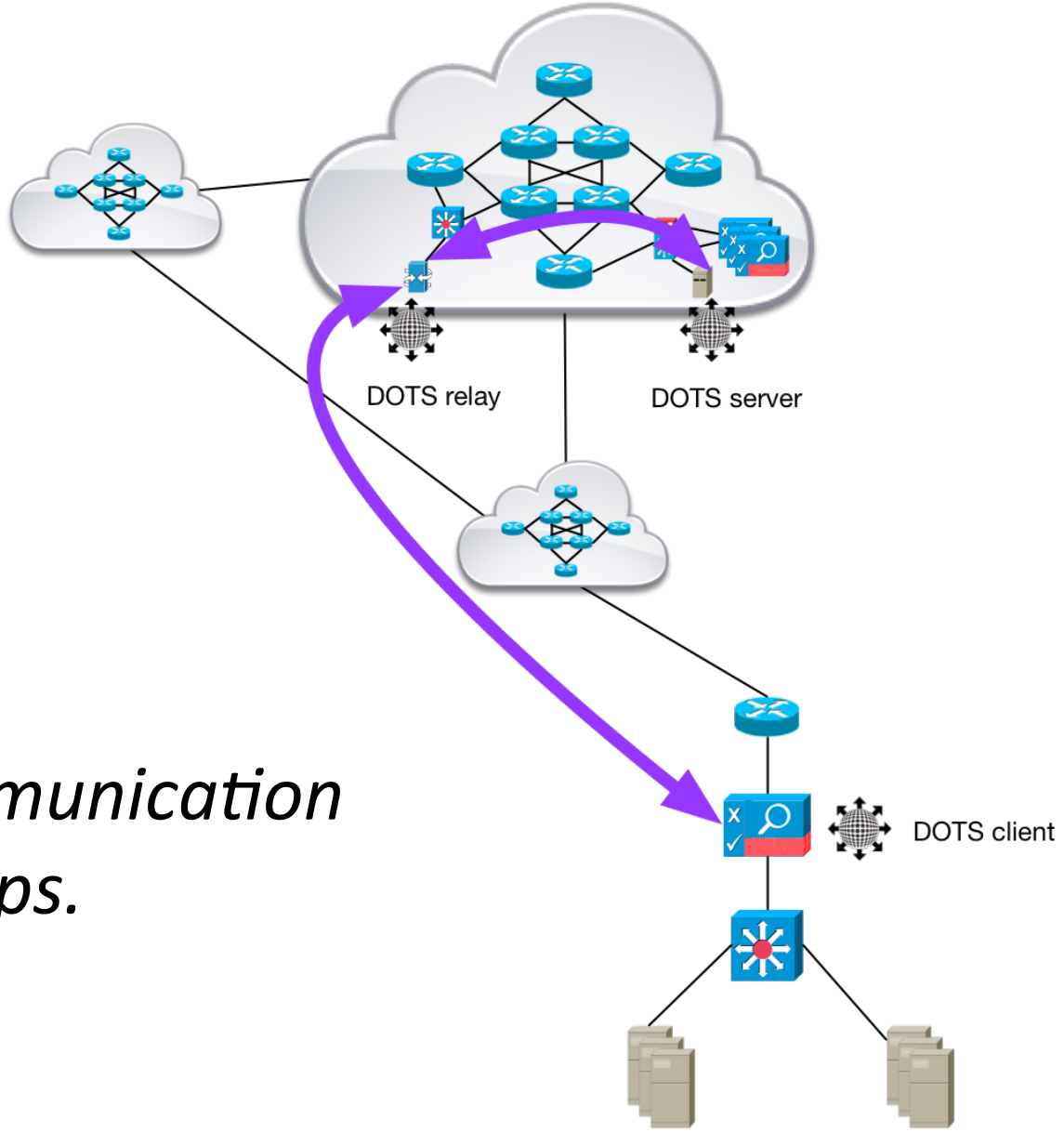


DOTS WG

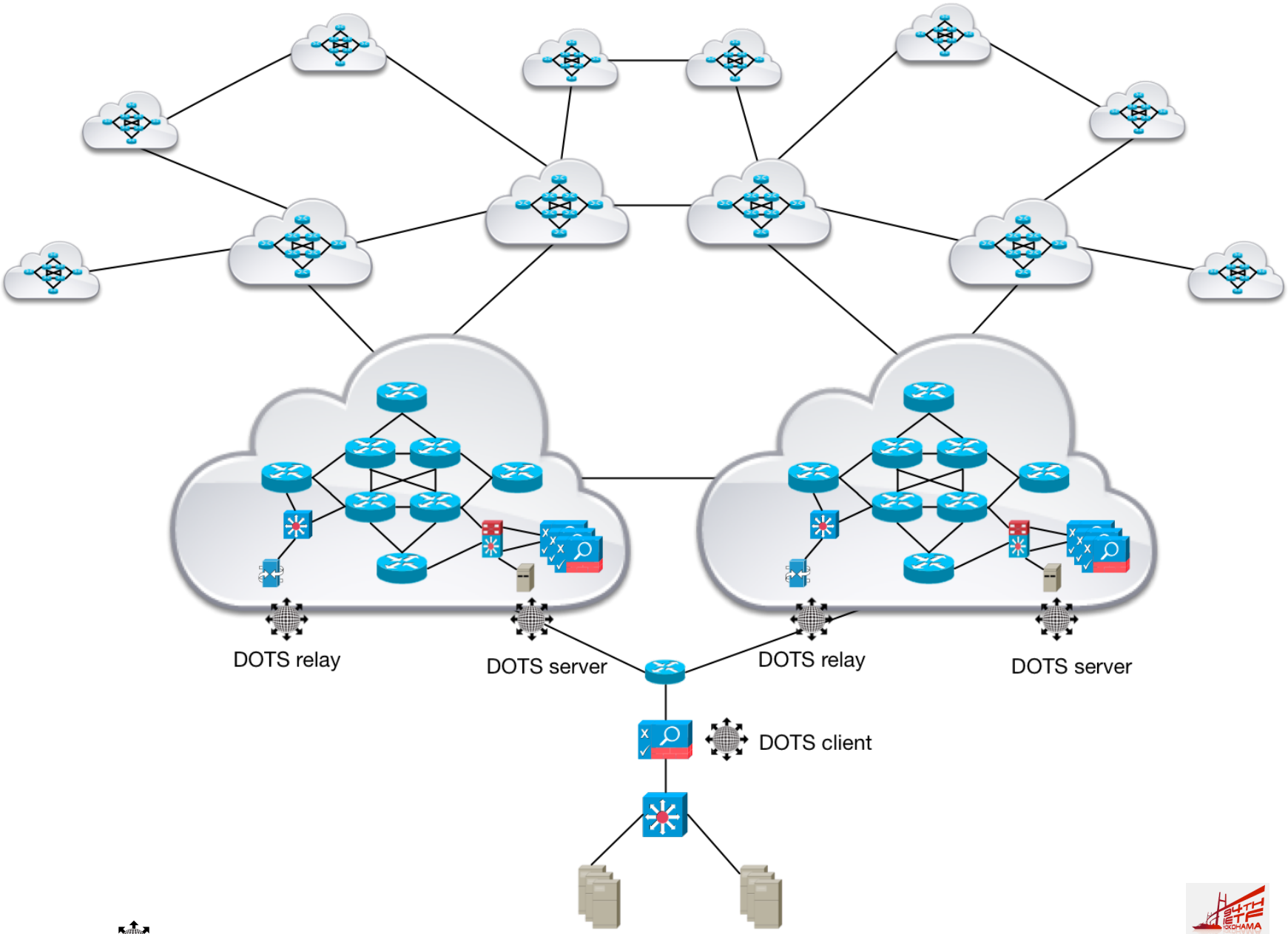


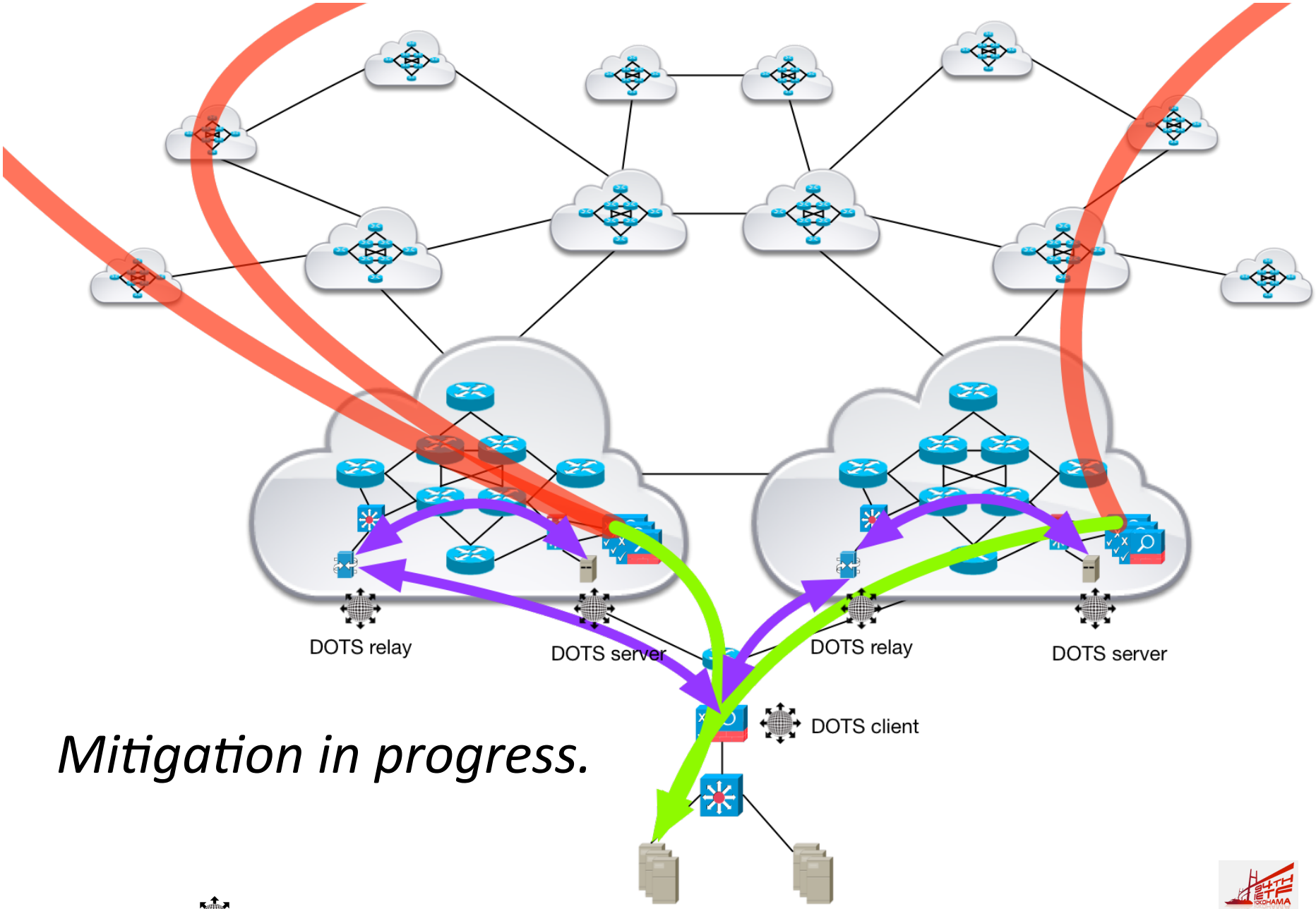
Mitigation in progress.

DOTS communication relationships.

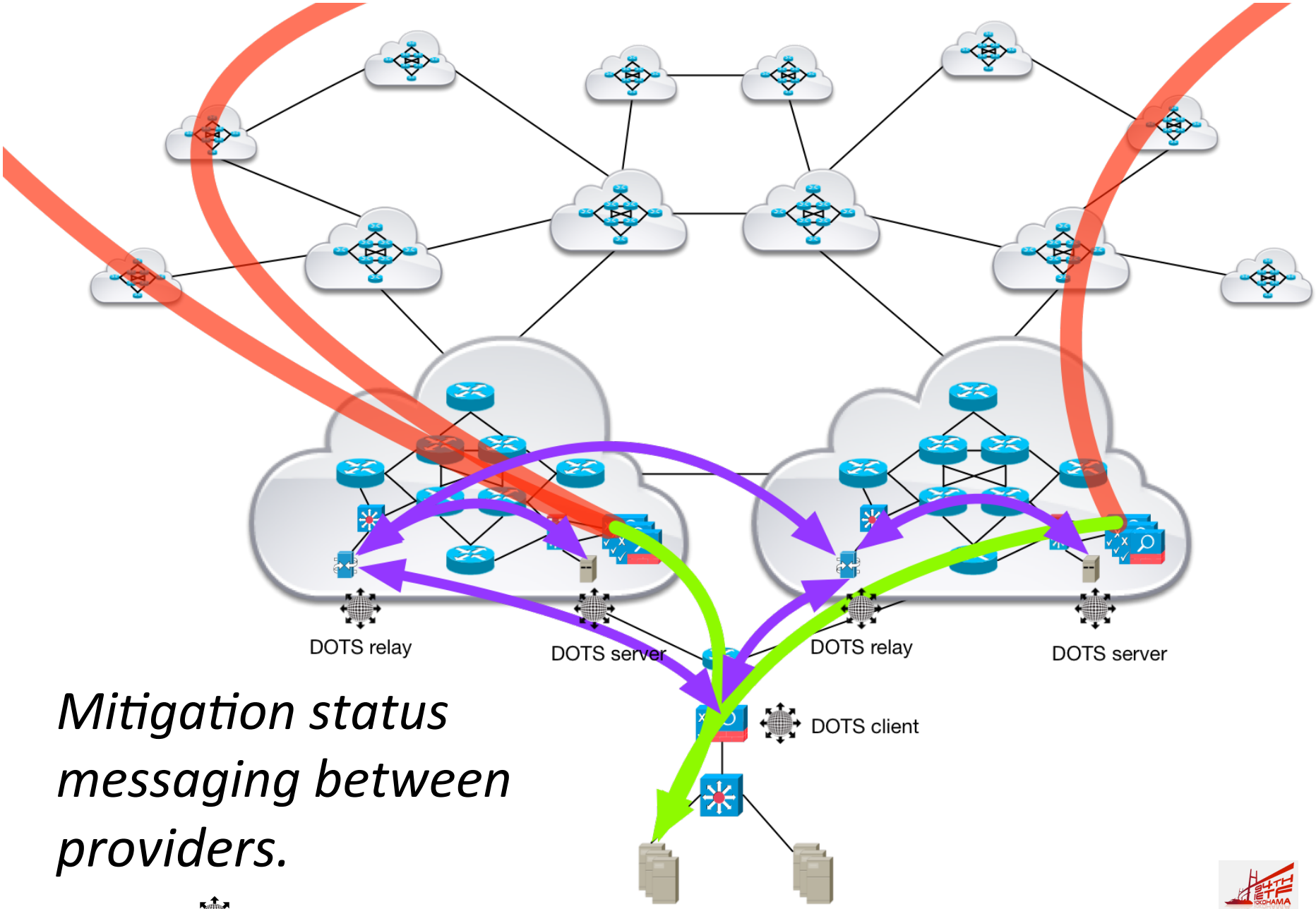


4.1.1 – Variation with Multiple Upstream DDoS Mitigation Providers

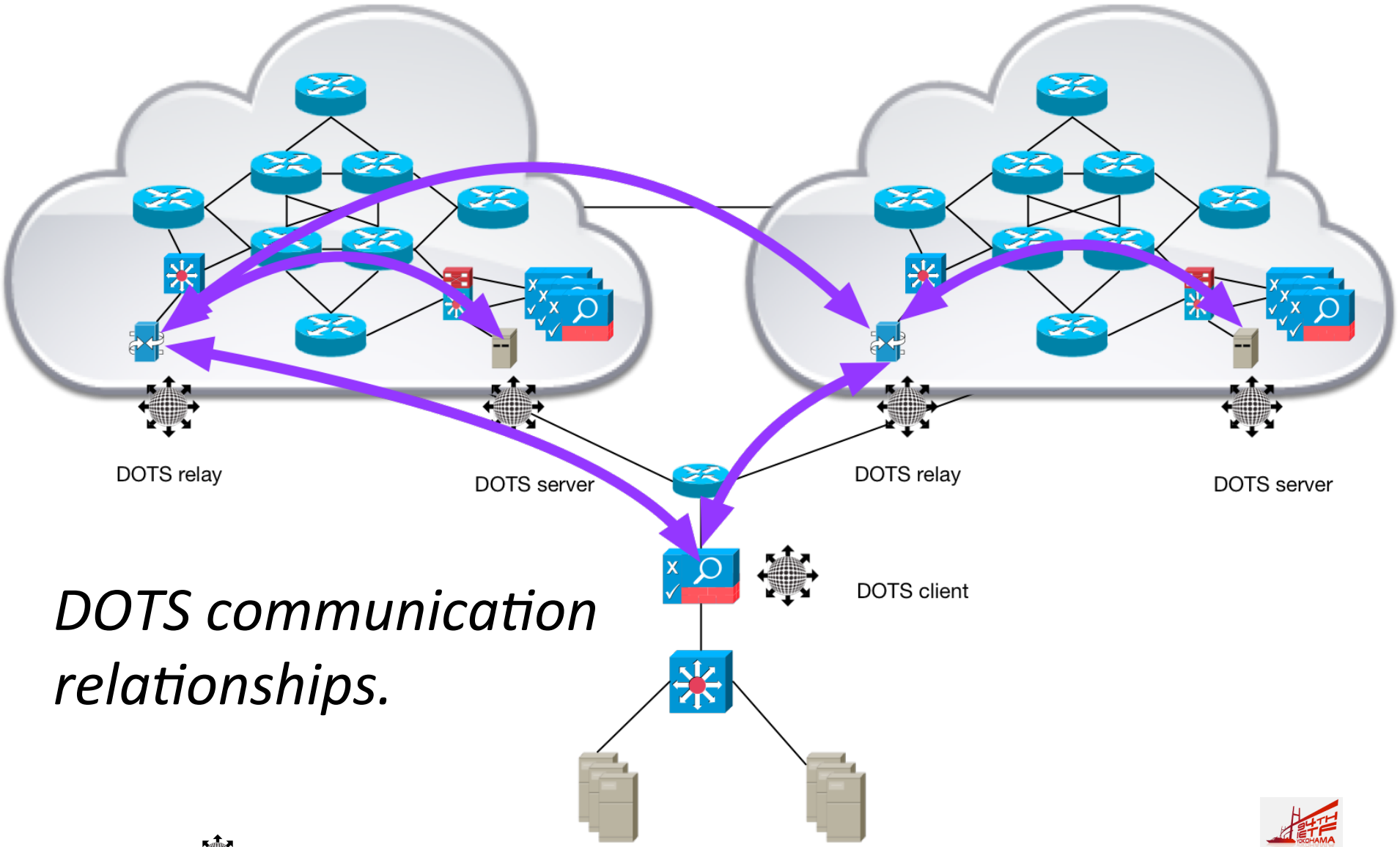

DOTS relay
DOTS server
DOTS relay
DOTS server
DOTS client



Mitigation in progress.

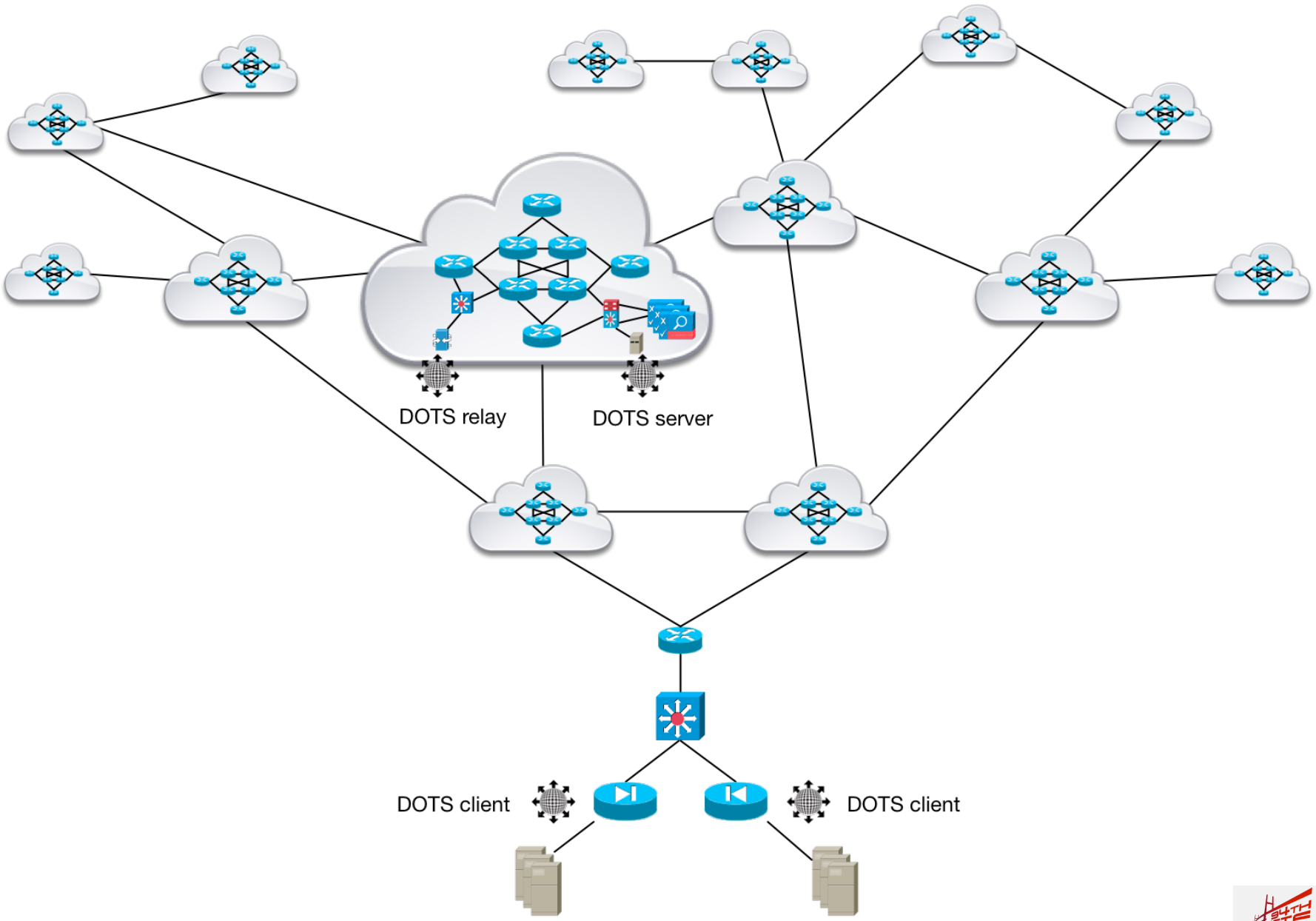


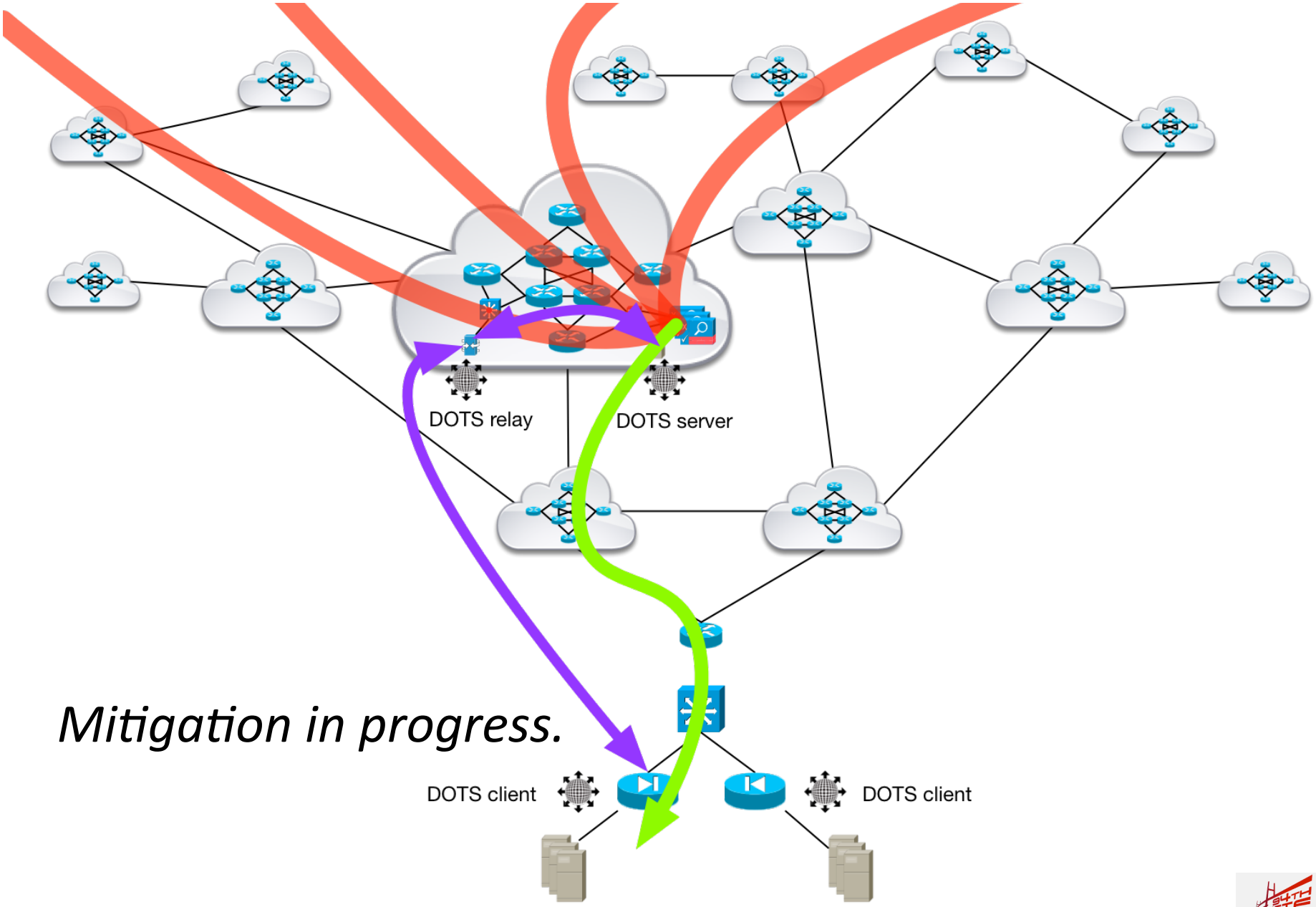
Mitigation status messaging between providers.



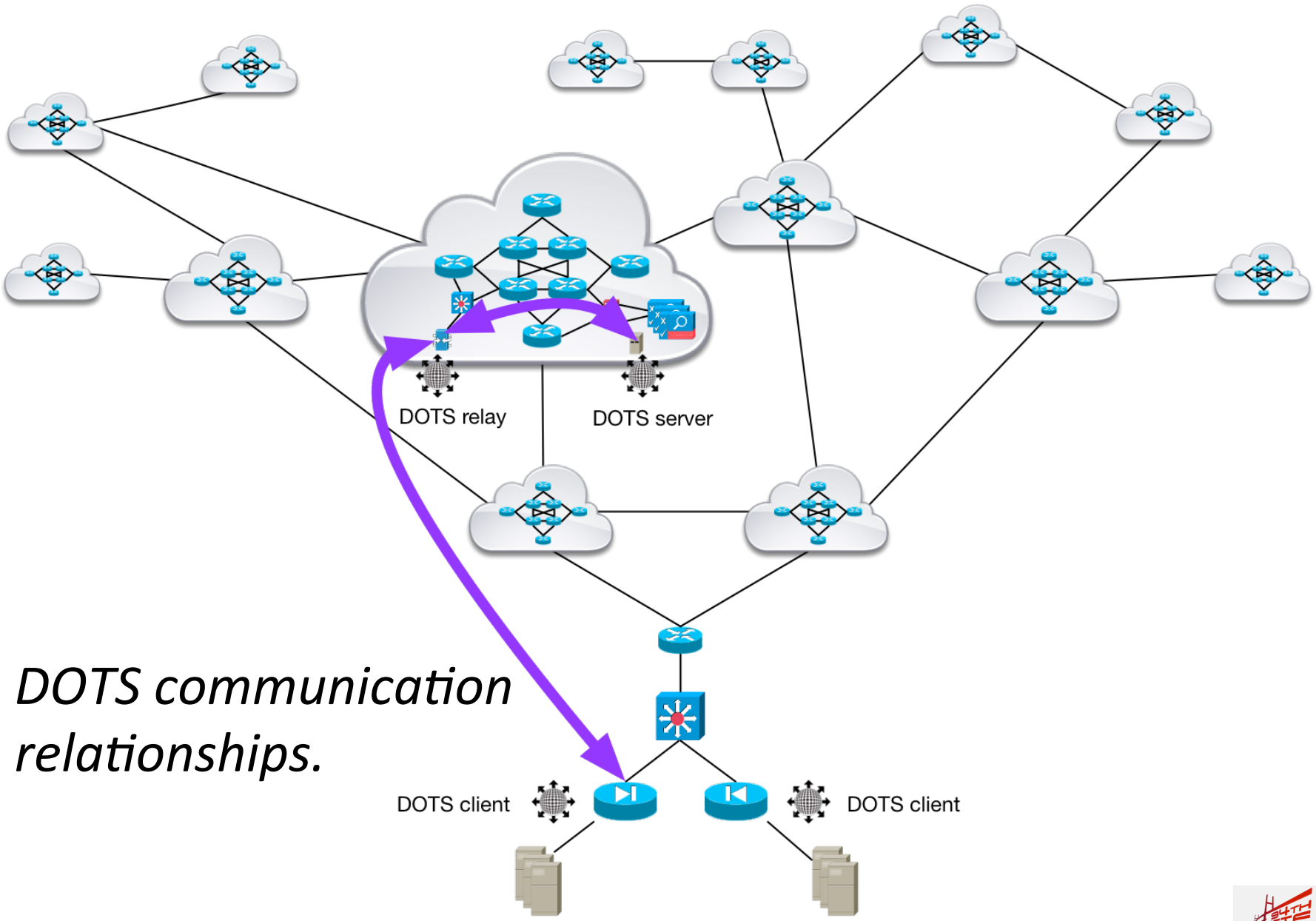
DOTS communication relationships.

4.1.2 – Network Infrastructure Device Requests Upstream DDoS Mitigation


DOTS relay
DOTS server
DOTS client
DOTS client

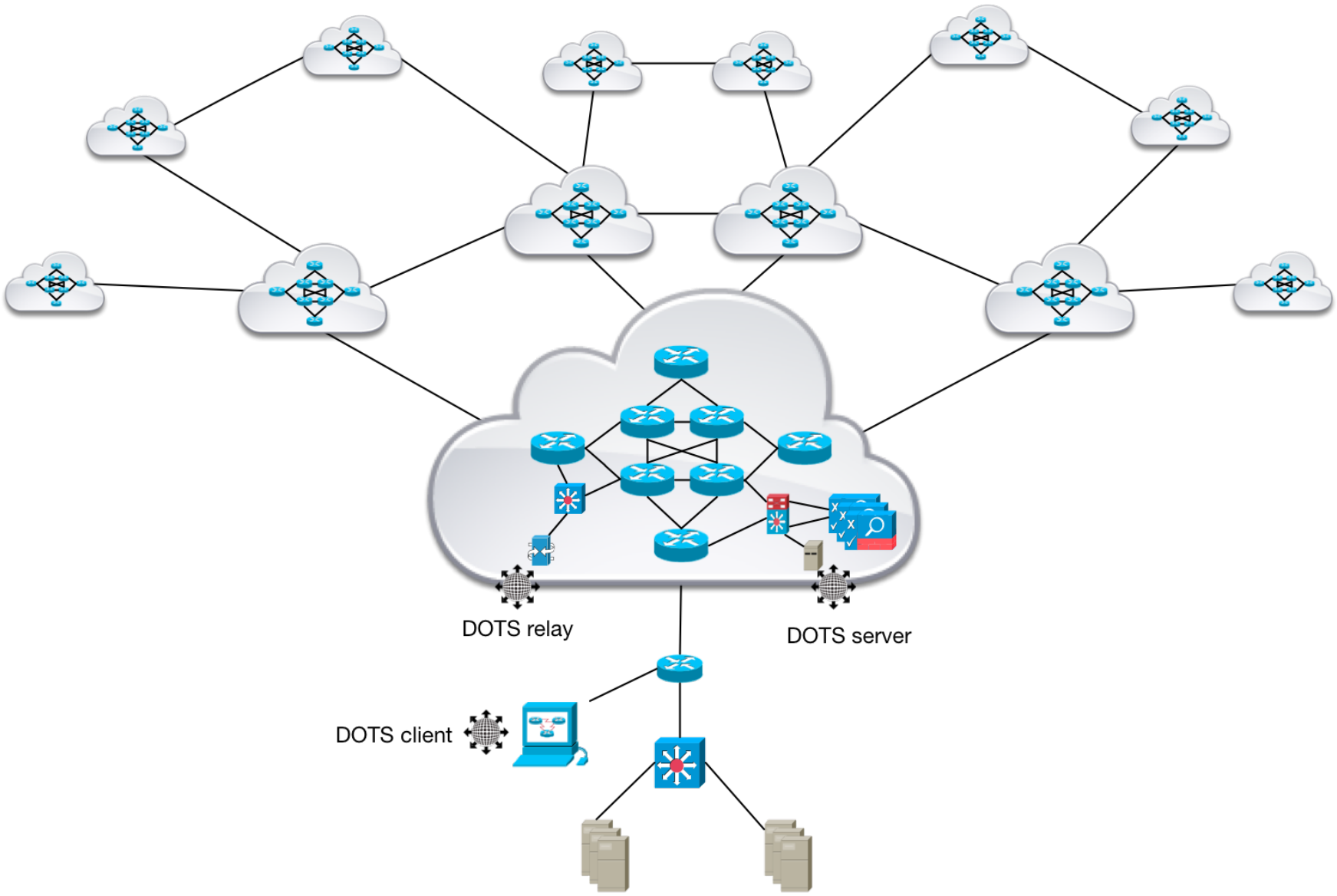


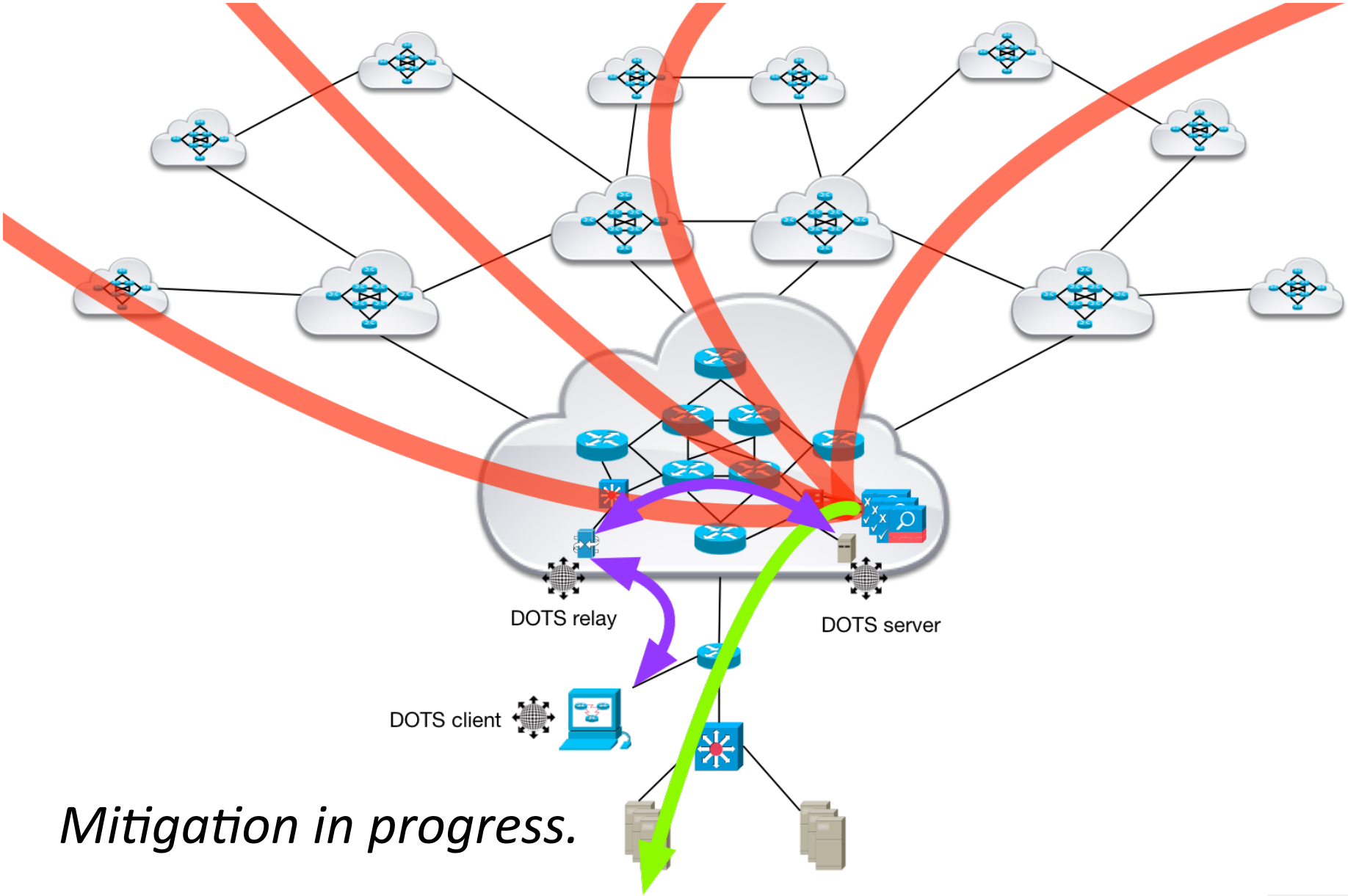
Mitigation in progress.



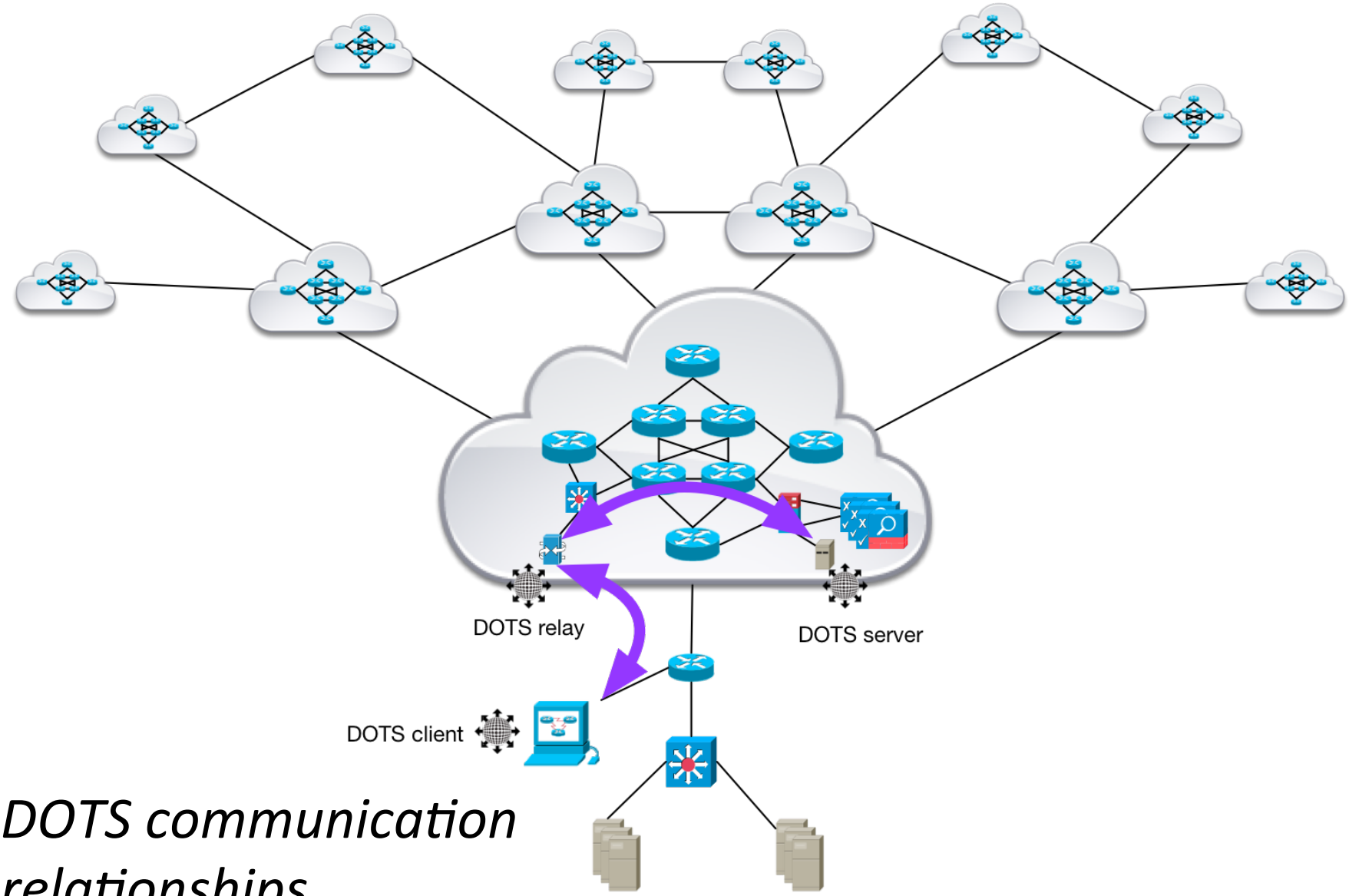
DOTS communication relationships.

4.1.3 – Attack Telemetry Detection/ Classification System Requests Upstream DDoS Mitigation


DOTS relay
DOTS server
DOTS client

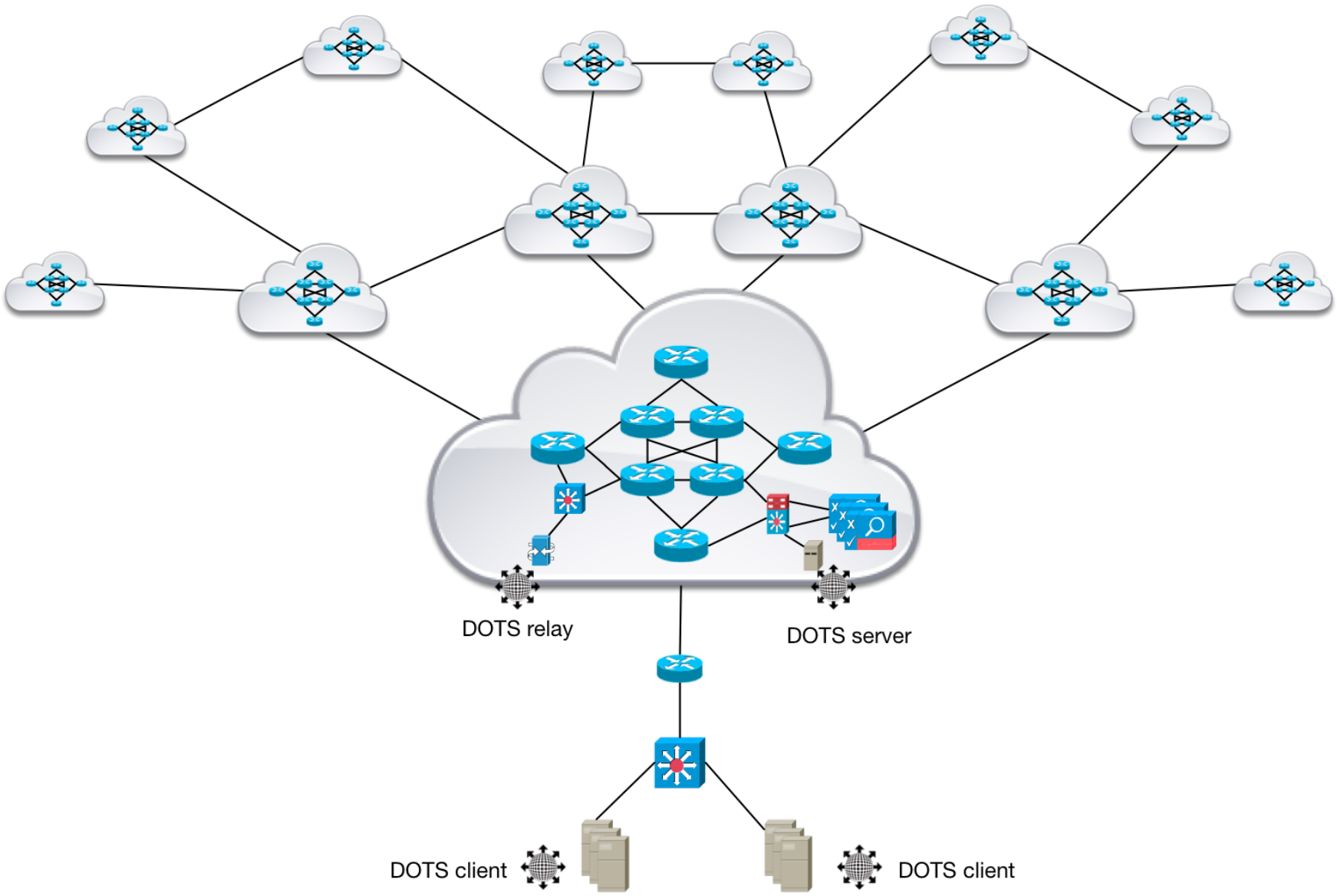


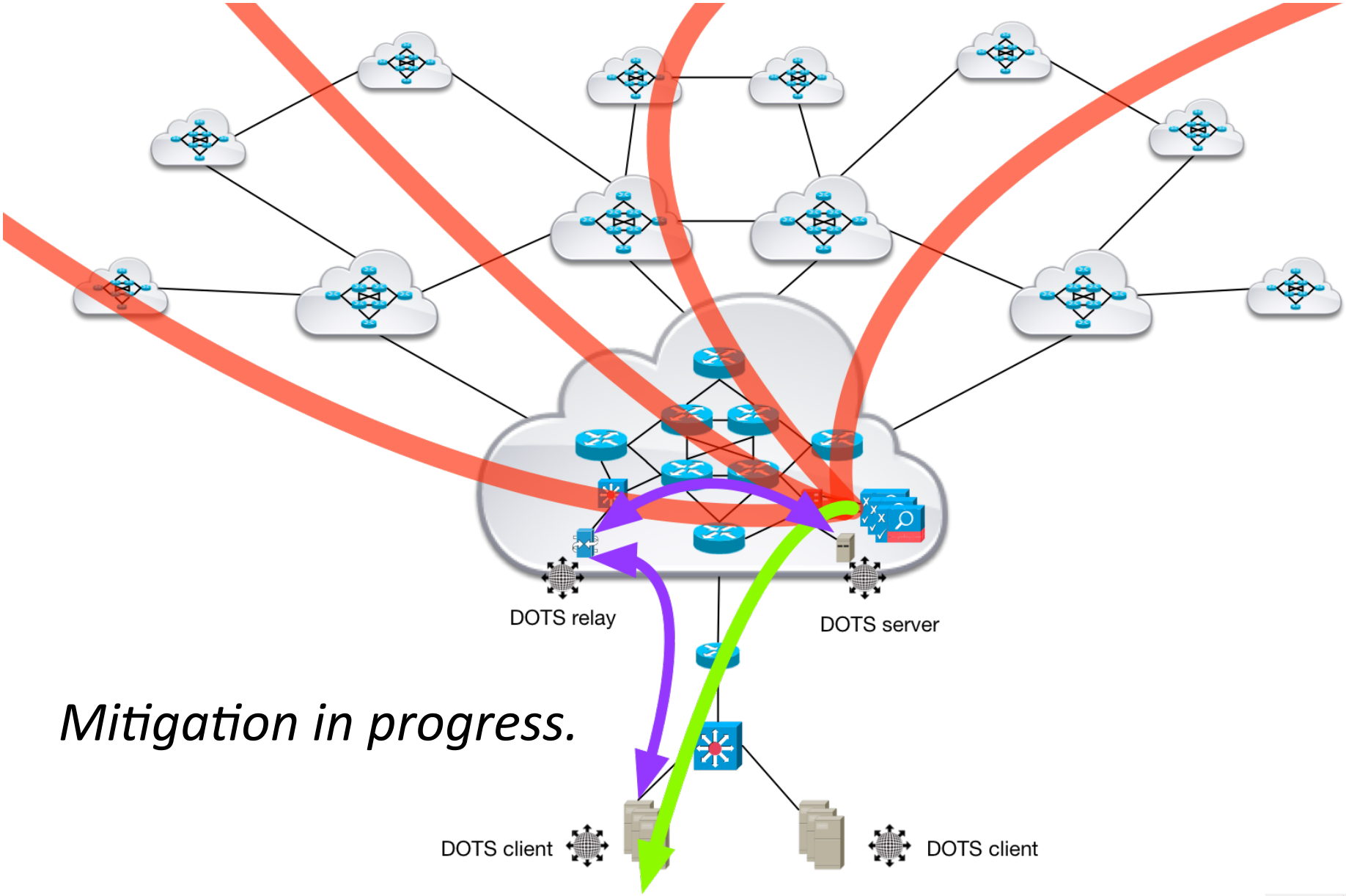
Mitigation in progress.



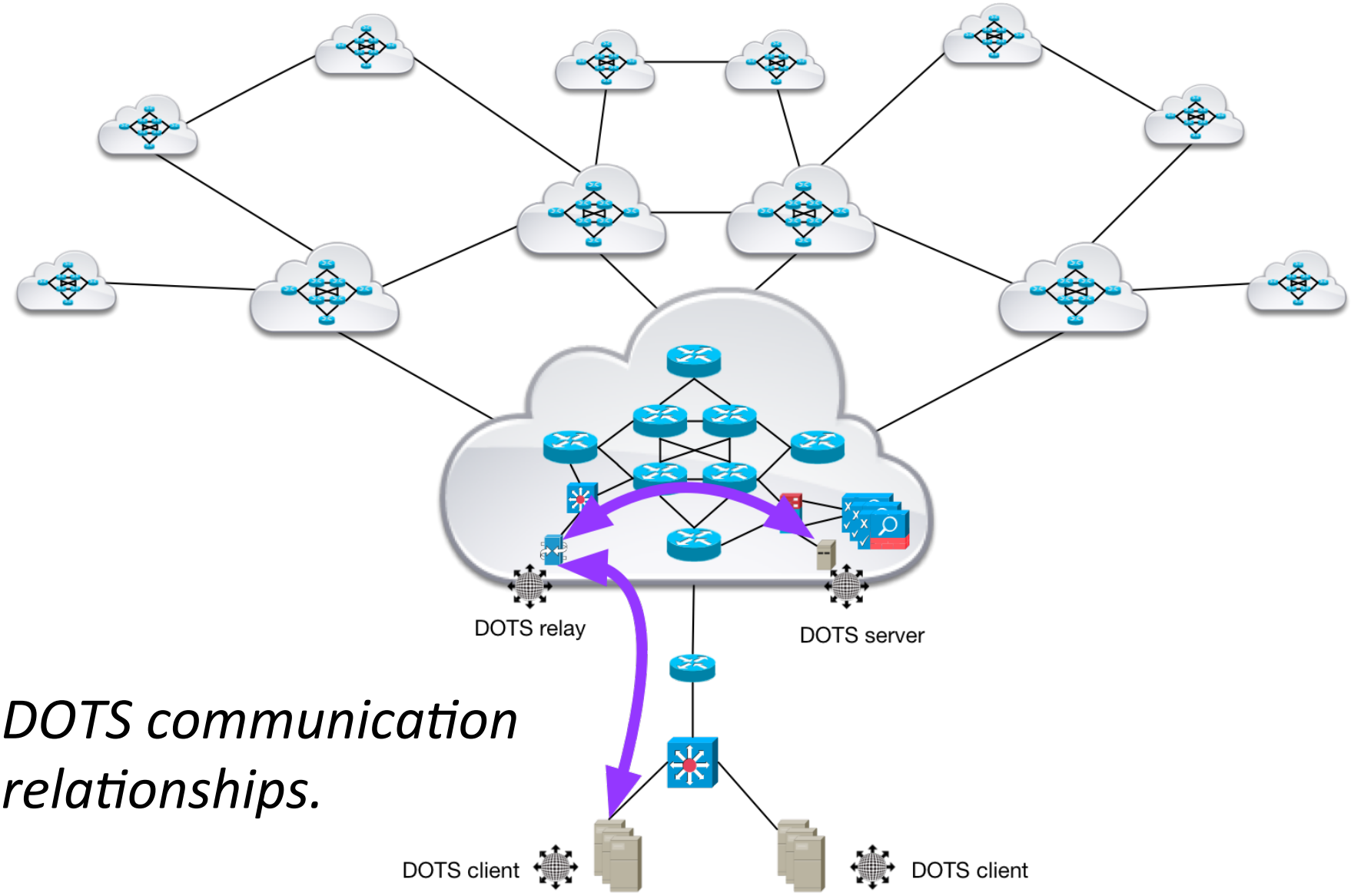
DOTS communication relationships.

4.1.4 – Targeted Service/Application Requests Upstream DDoS Mitigation


DOTS relay
DOTS server
DOTS client
DOTS client

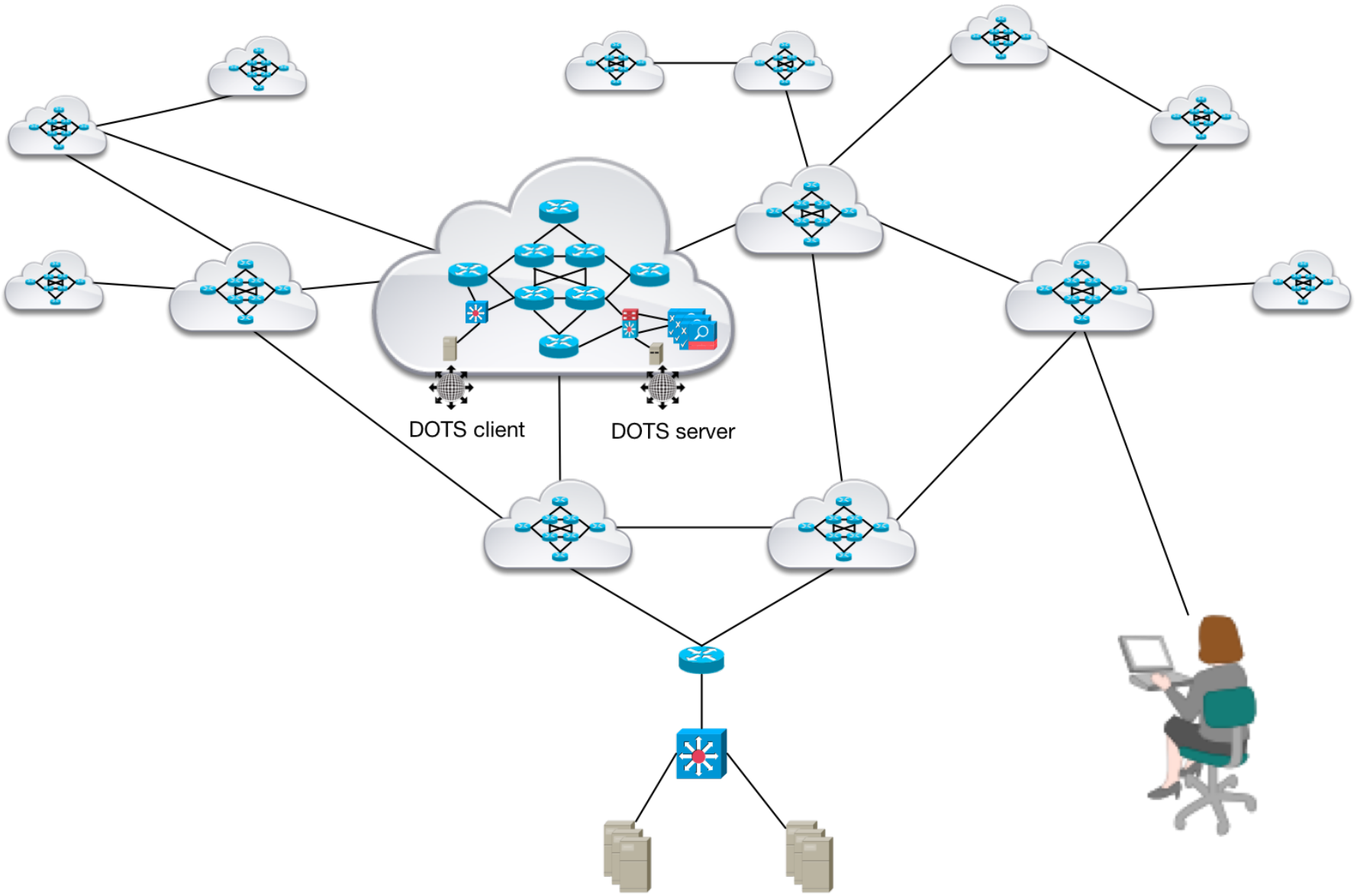


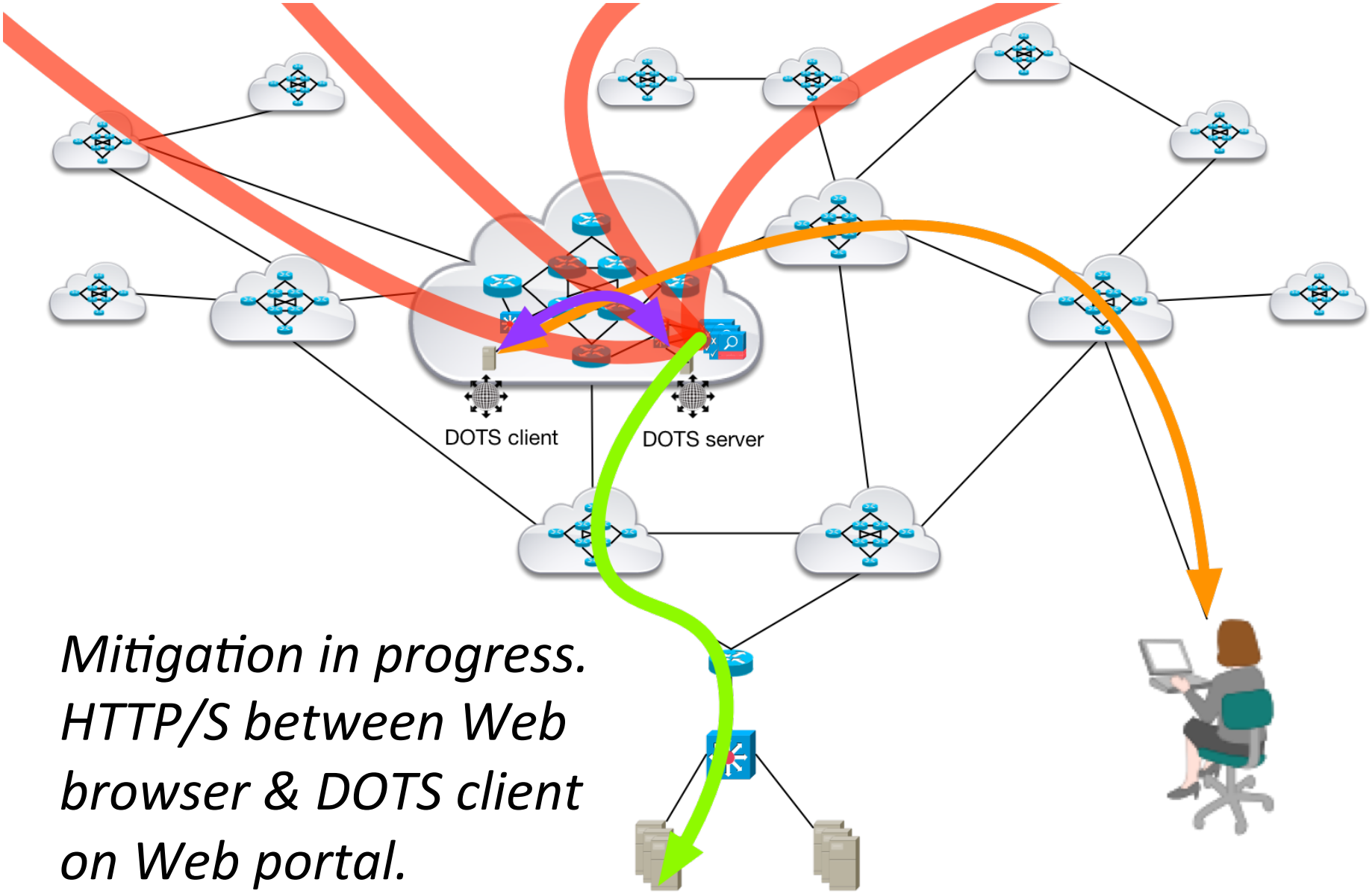
Mitigation in progress.



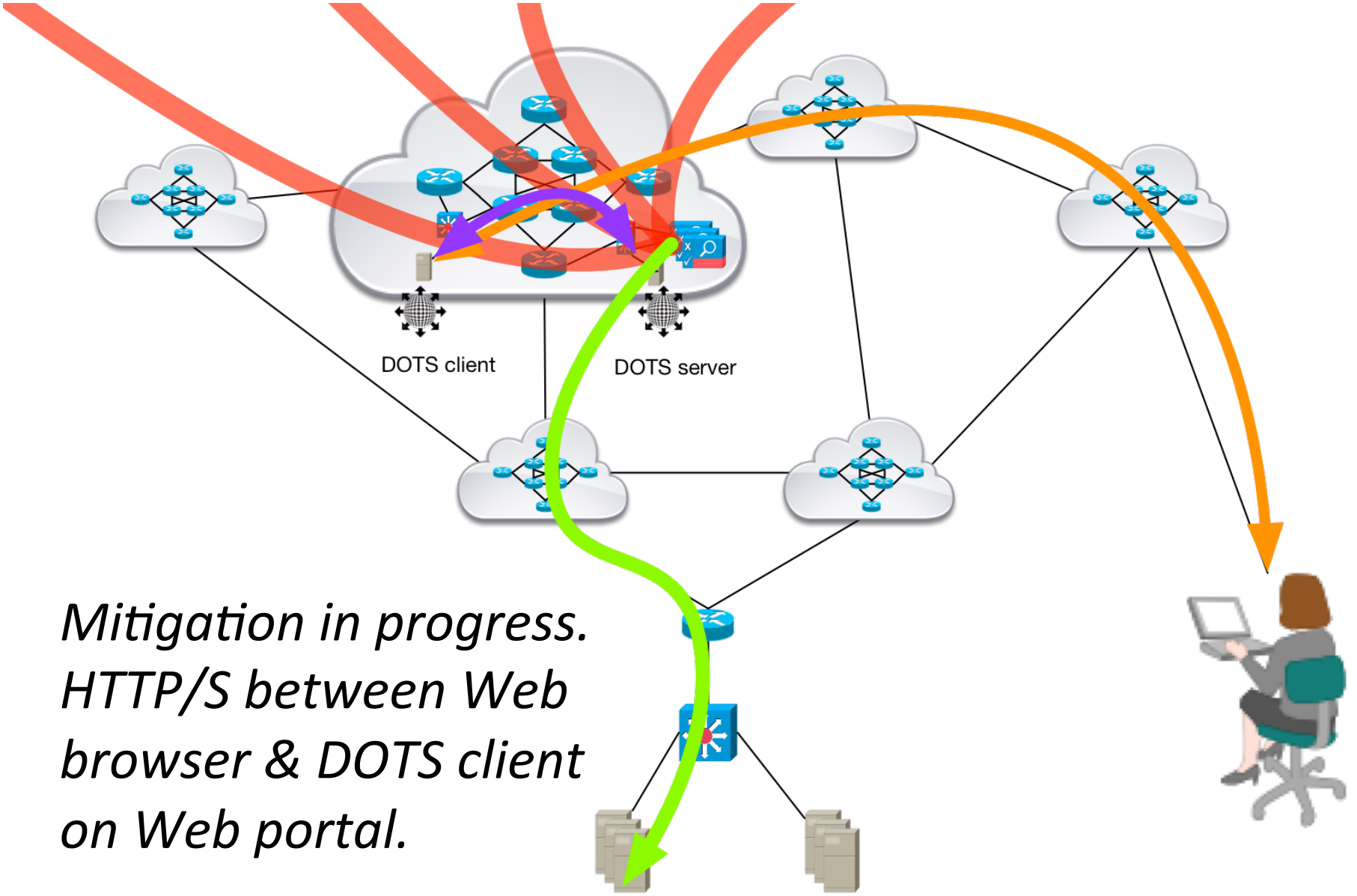
DOTS communication relationships.

4.1.5 – Manual Web Portal Request to Upstream Mitigator

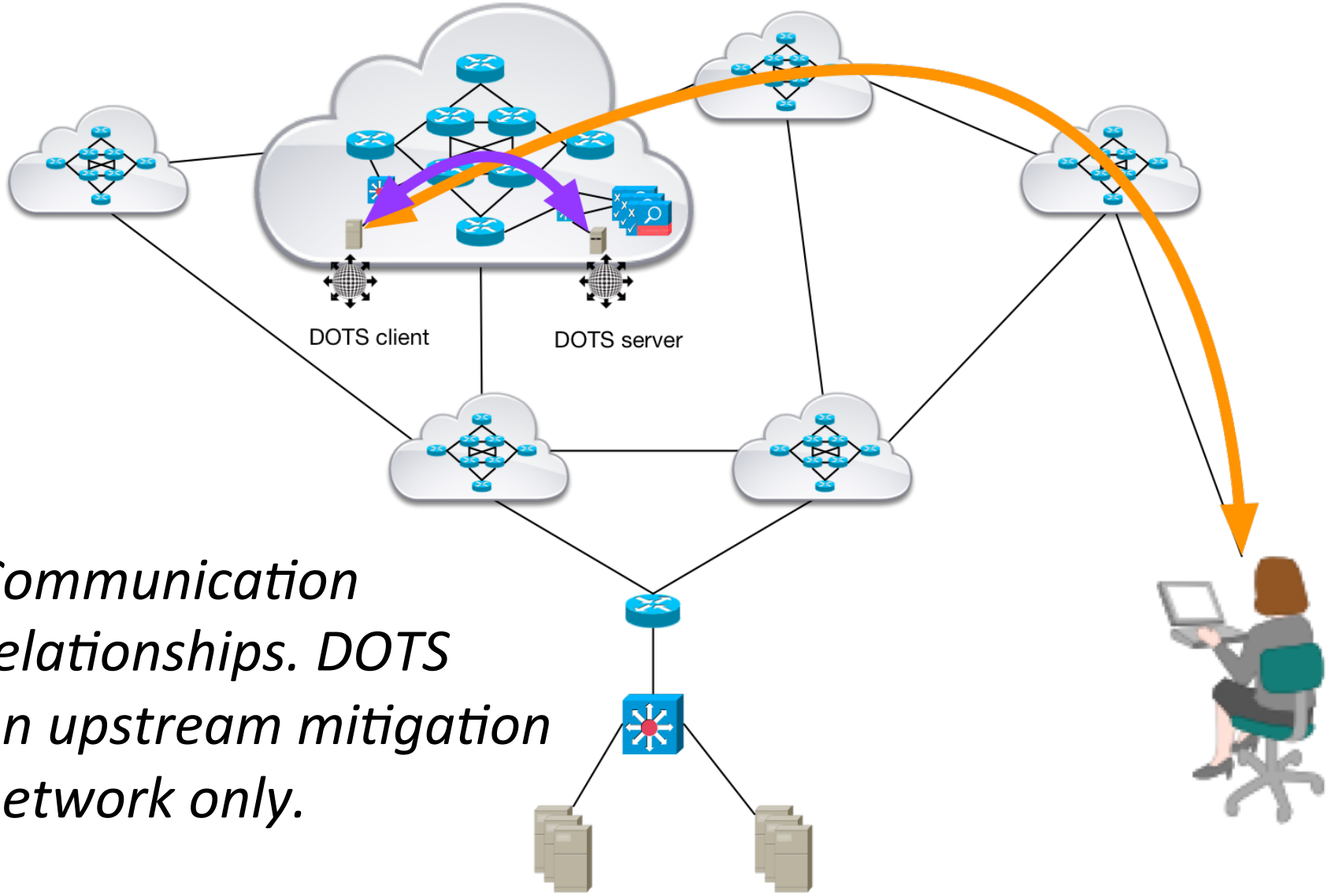

DOTS client
DOTS server



Mitigation in progress. HTTP/S between Web browser & DOTS client on Web portal.

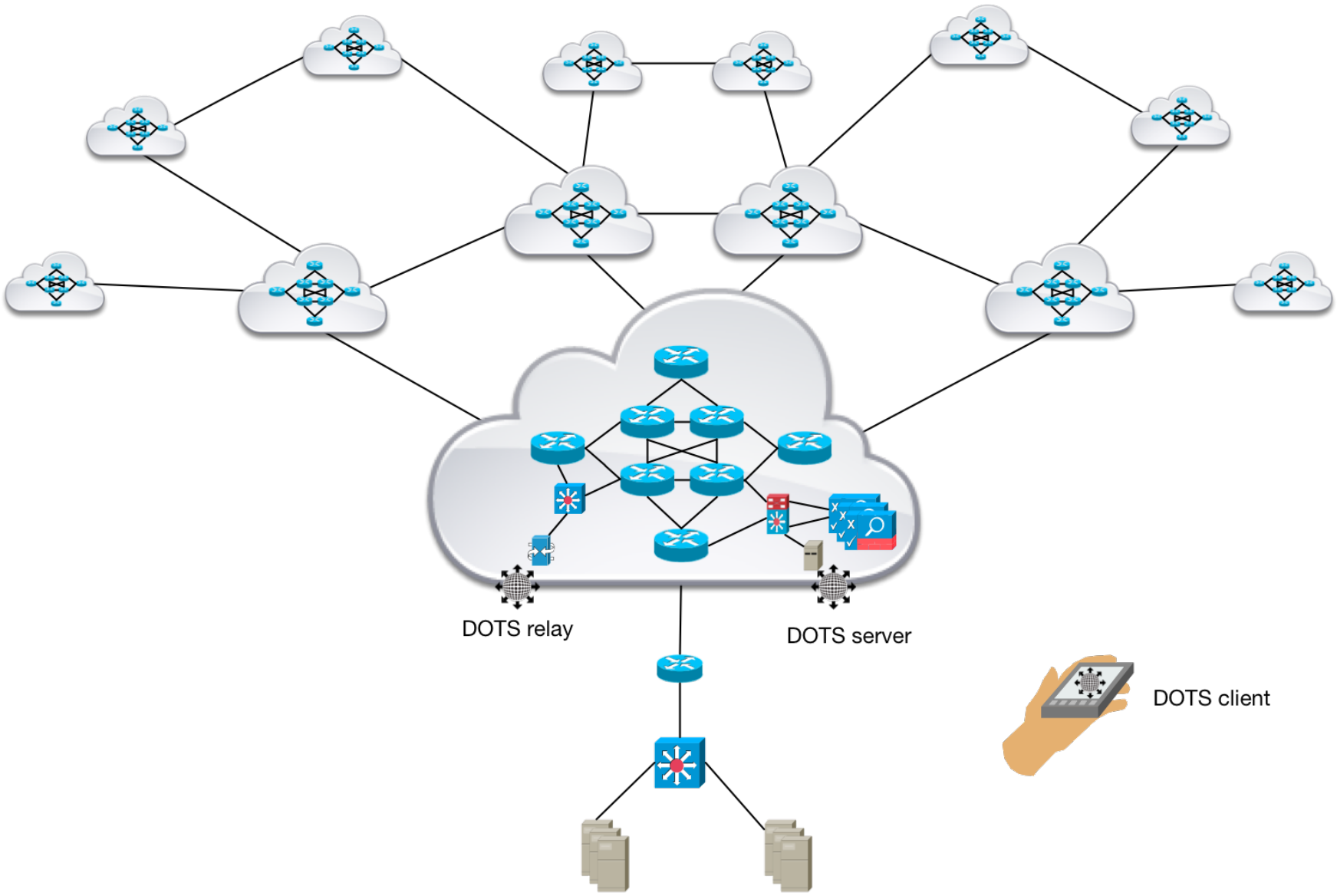


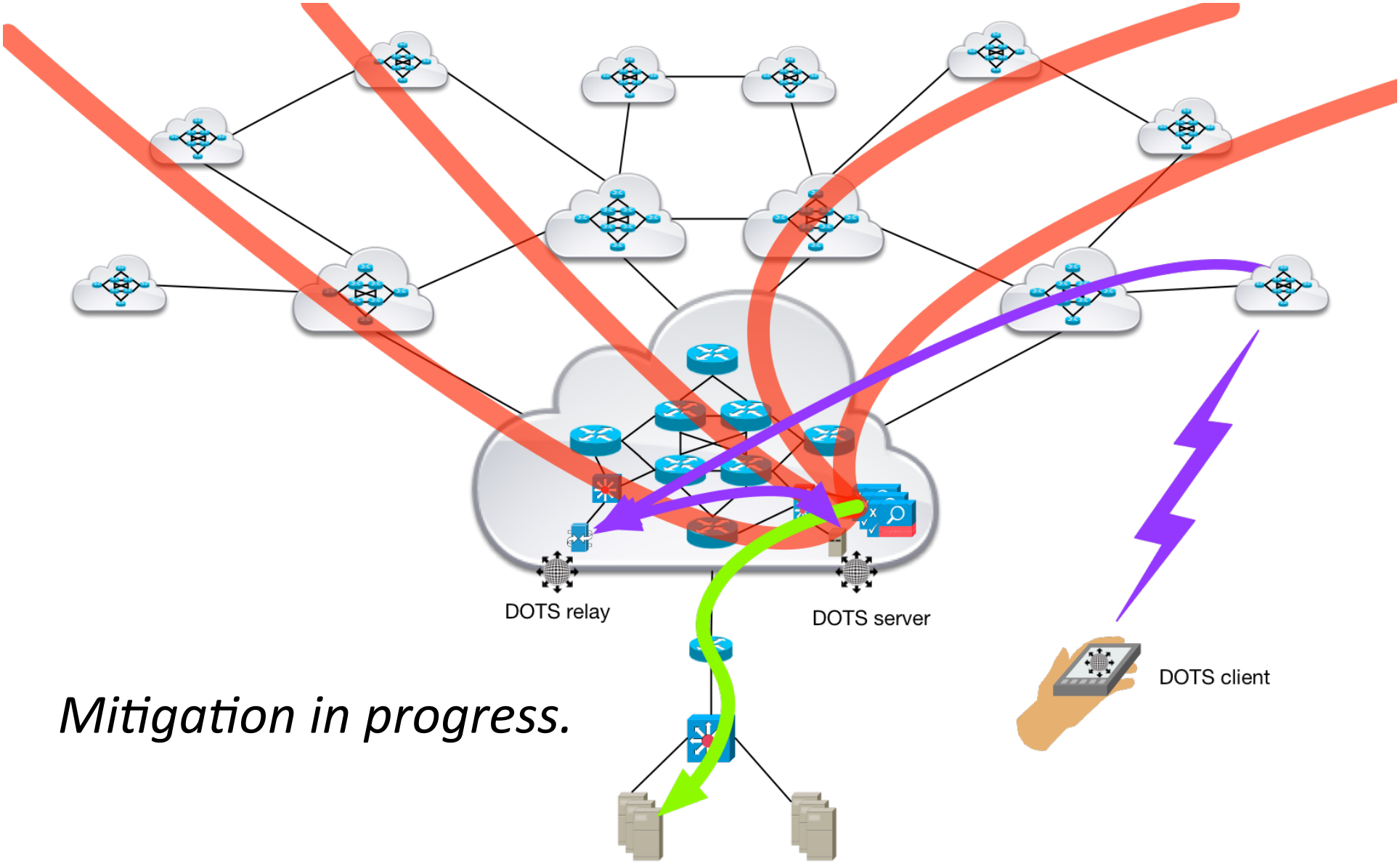
Mitigation in progress. HTTP/S between Web browser & DOTS client on Web portal.



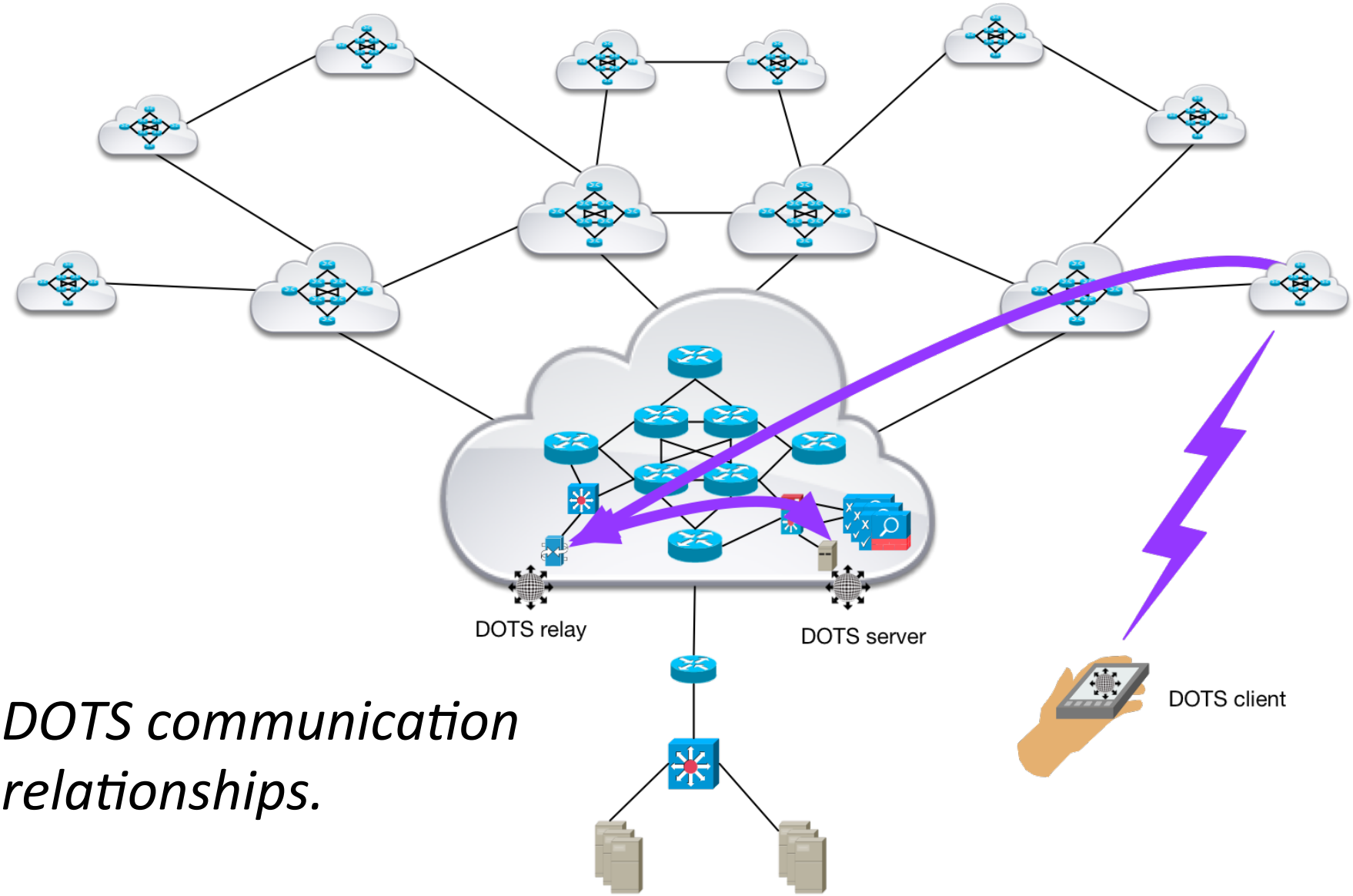
Communication relationships. DOTS on upstream mitigation network only.

4.1.6 – Manual Mobile Device Application Request to Upstream Mitigator


DOTS relay
DOTS server
DOTS client

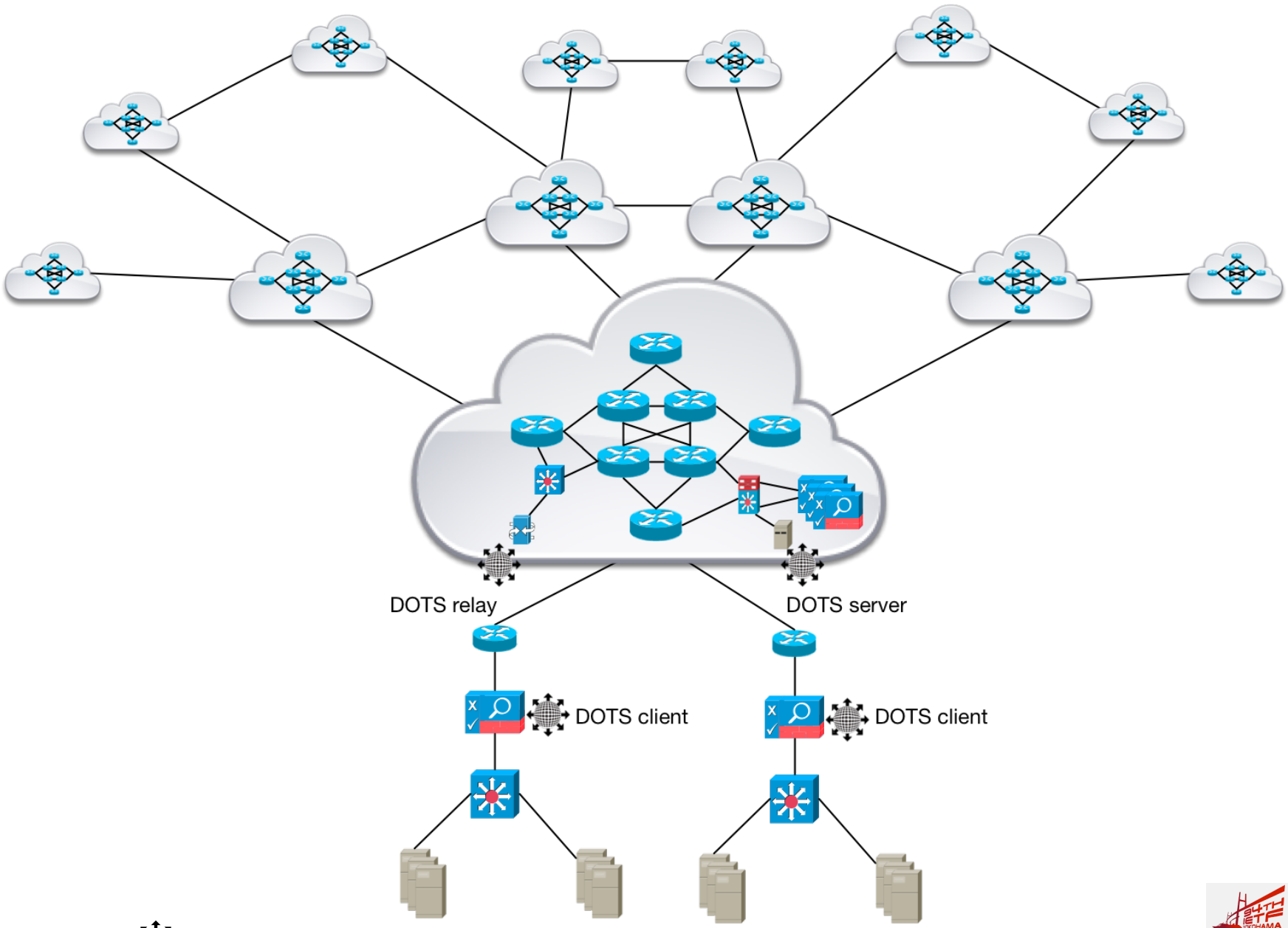


Mitigation in progress.

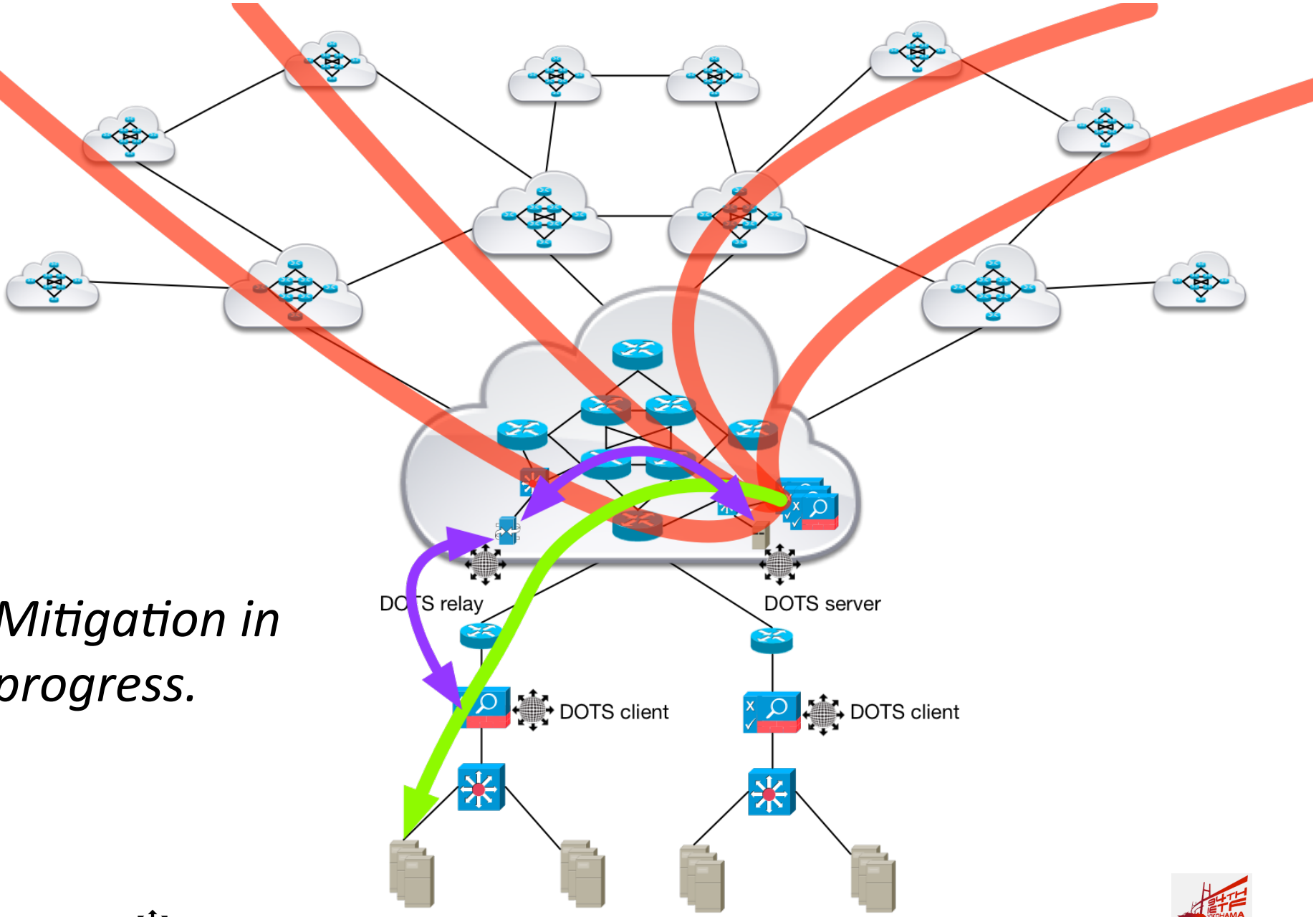


DOTS communication relationships.

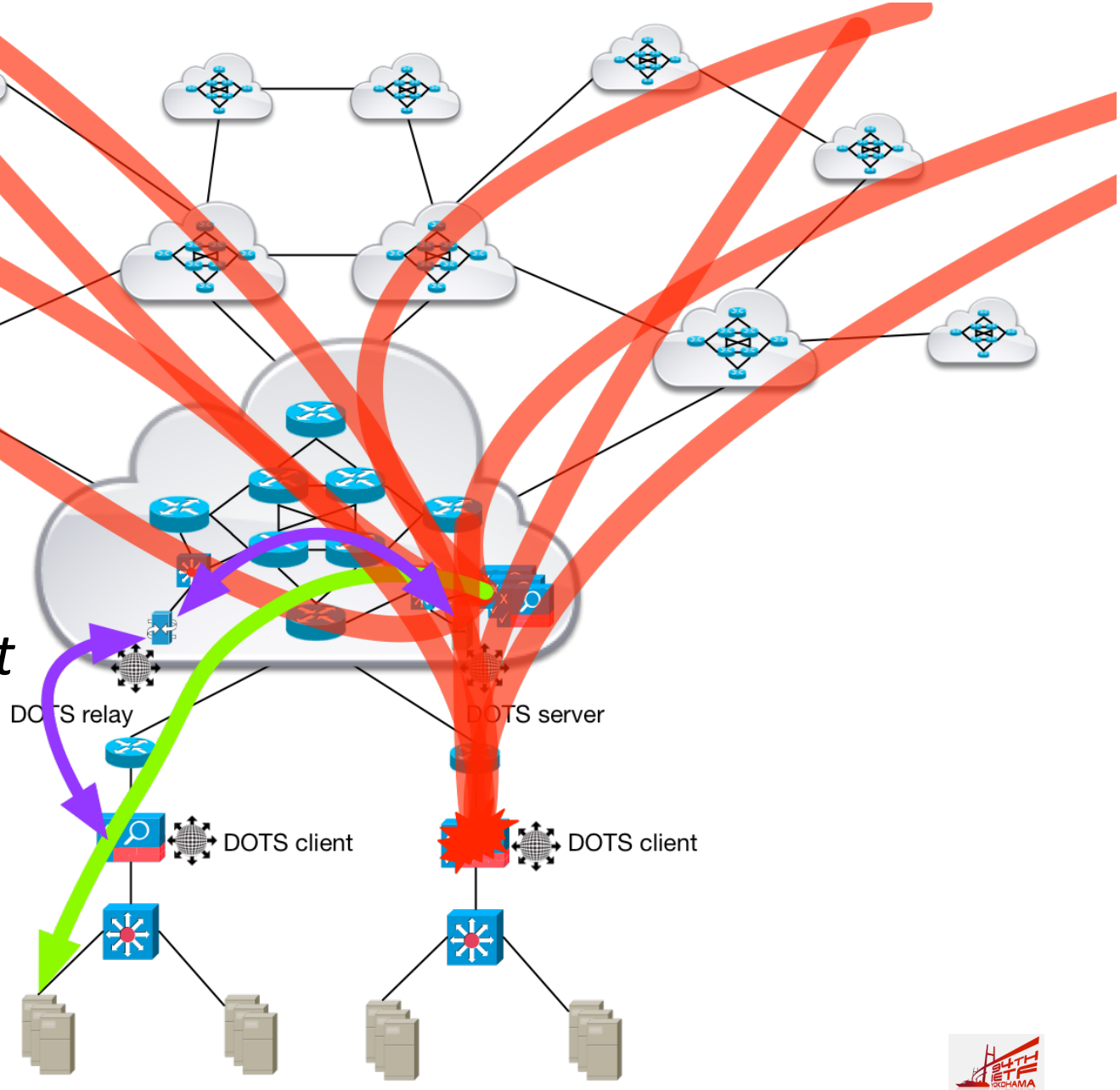
4.1.7 – Unsuccessful CPE or PE Mitigator Request for Upstream DDoS Mitigation

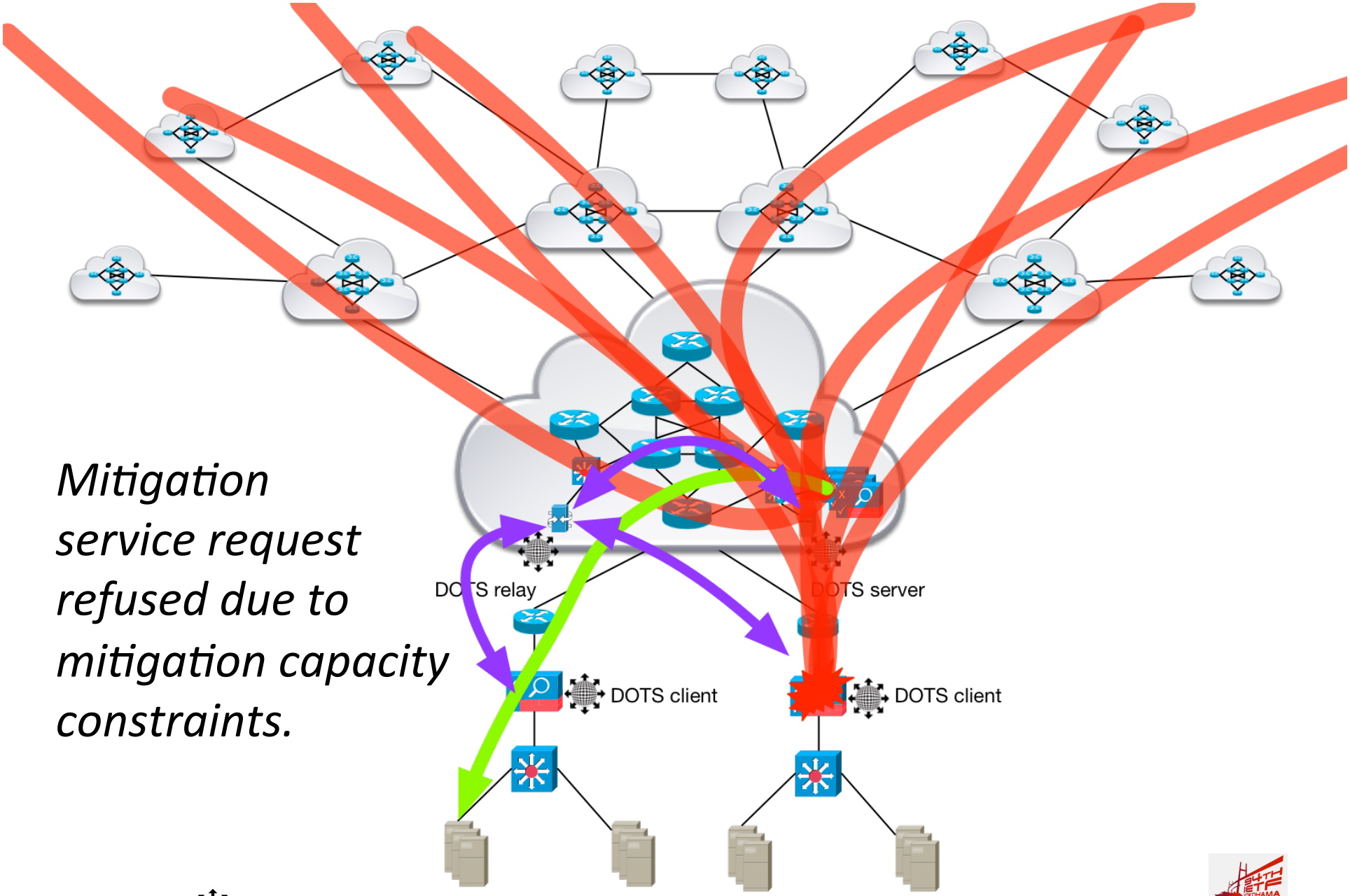

DOTS relay
DOTS server
DOTS client
DOTS client

Mitigation in progress.

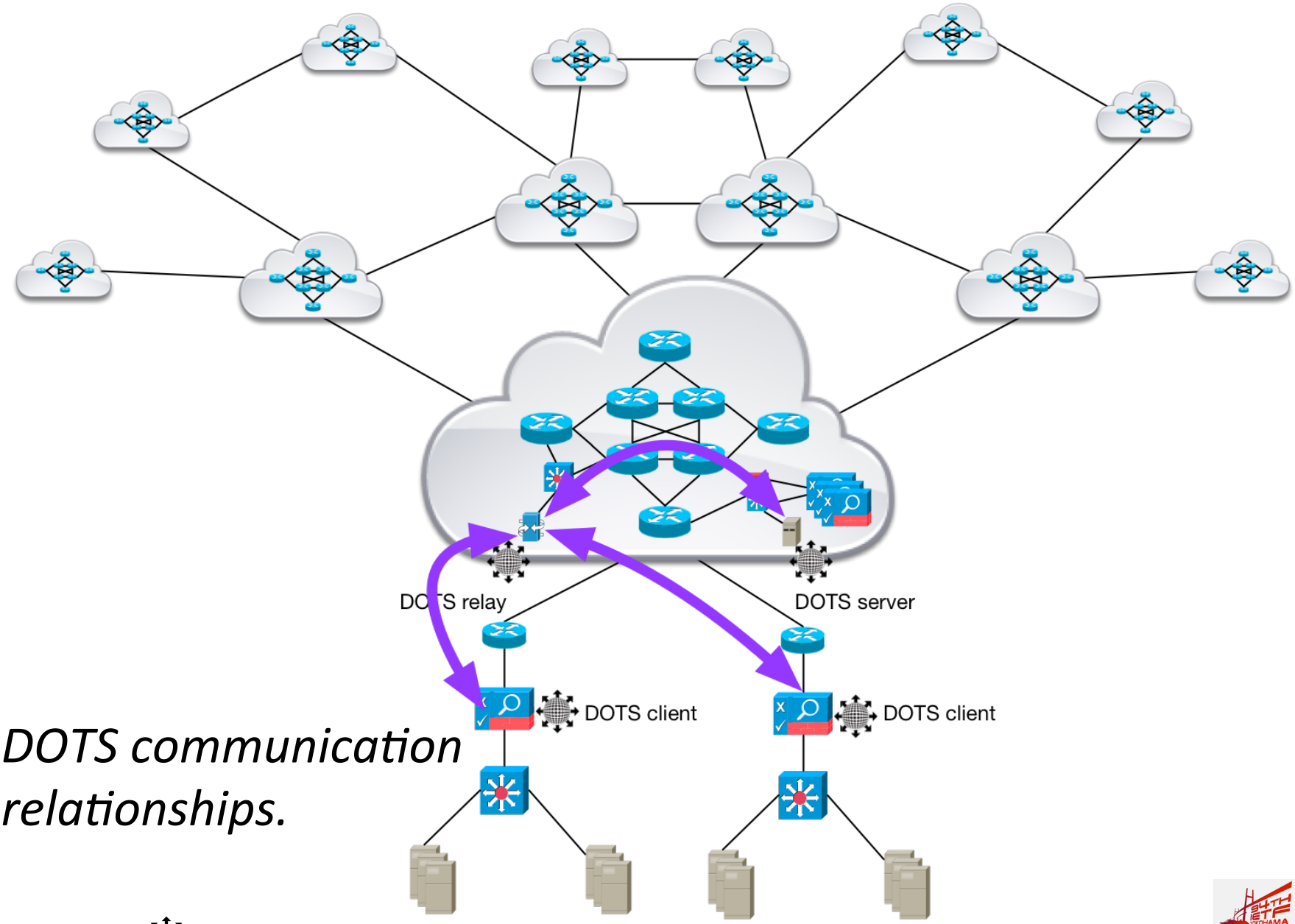


Another attack initiated, different target.





Mitigation service request refused due to mitigation capacity constraints.



DOTS communication relationships.

4.2 - Ancillary Use Cases

4.2.1 – Auto-Registration

- Beyond attack mitigation requests, responses, and status messages, DOTS can also be useful for administrative tasks.
- Administrative tasks are a significant barrier to effective DDoS mitigation.
- DOTS clients with appropriate credentials can auto-register with DOTS servers on upstream mitigation networks.
- This helps with DDoS mitigation service on-boarding, moves/adds/changes.

4.2.2 – Automatic Provisioning of DDoS Countermeasures

- DDoS countermeasure provisioning today is a largely manual process, errors and inefficiency can be problematic.
- This can lead to inadequately-provisioned DDoS mitigation services which often are not optimized for the assets under DDoS protection. Mitigation rapidity, efficacy suffers.
- On-boarding organizations during an attack – an all-too-common situation – can be very challenging.
- The 'self-descriptive' nature of DOTS registration and mitigation status requests can be leveraged to automate the countermeasure selection, provisioning, and tuning process.
- Mitigation efficacy feedback from DOTS clients to DOTS servers during an attack can be leveraged for real-time mitigation tuning and optimization.

4.2.3 – Informational DDoS Attack Notification to Third Parties

- In addition to service requests from organizations under attack to upstream mitigators, DOTS can be used to send DDoS attack notification and status messages to interested and authorized third parties.
- It may be beneficial in some circumstances to automatically provide attack notifications and status messages econdary or tertiary ‘backup’ mitigation providers, security researchers, vendors, law enforcement agencies, regulatory agencies, etc.
- Any such sharing of information with third parties should only take place in accordance with all relevant laws, regulations, contractual obligations, privacy and confidentiality agreements.

Next Steps for Use-Cases Draft

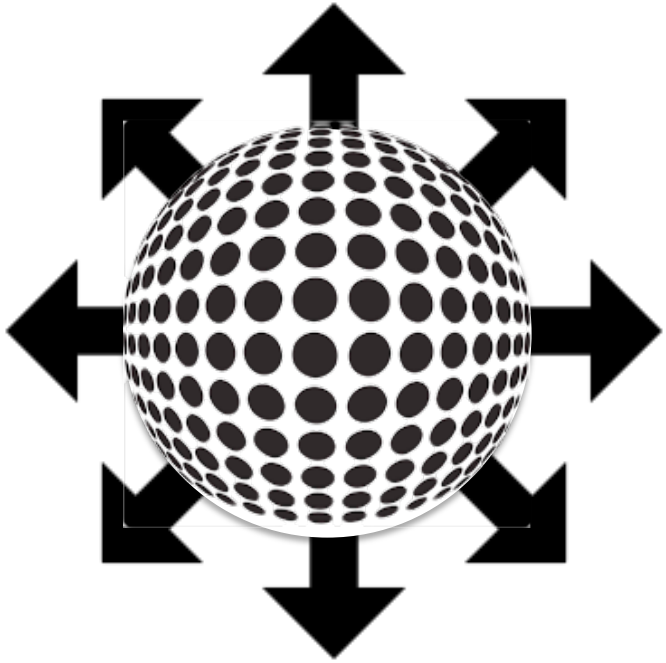
To-Do List for draft-dots-ietf-use-cases-01

- Fix typos (doh!).
- Remove duplicative verbiage.
- Wordsmith phrasing for clarity.
- Present use-cases via ‘diffs’ – i.e., refer to commonalities with other use-cases, emphasize specific factors unique to each use-case.
- Reconcile definitions of terminology with dots-ietf-requirements draft.
- Add use-cases illustrating suppression of DDoS attack traffic on origin networks, filtering on intermediate networks.
- Add use-cases illustrating specific PE-PE scenarios (e.g., ‘overflow’ requests for additional DDoS mitigation capacity, etc.).

Request for Feedback from WG Participants

- What should we add?
- What should we remove?
- What should we change?
- Should we include variations (via ‘diffs’) on each use-case similar to what was done with 4.1.1 in this presentation?
- Other input?

This Presentation – http://bit.ly/1N6u8za



DDoS Open Threat Signaling (DOTS) Working Group

Thank you!

Roland Dobbins – Arbor Networks

Stefan Fouant – Corero Network Security

Daniel Migault – Ericsson

Robert Moskowitz – HTT Consulting

Nik Teague – Verisign

Liang ‘Frank’ Xia – Huawei