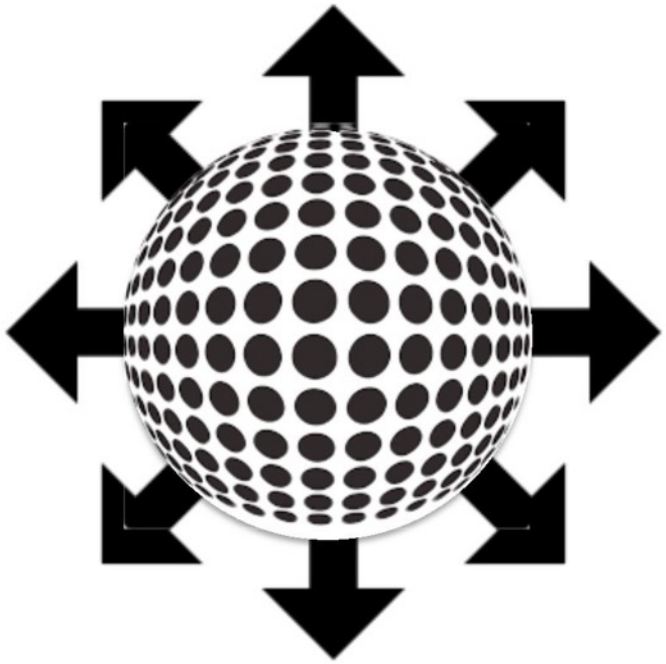


Amenaza abierta DDoS Señalización (DOTS) Grupo de trabajo

borrador-ietf-dots-use-cases-00

Roland Dobbins - Arbor Networks

Stefan Fouant - Corero Network Security

Daniel Migault – Ericsson

Robert Moskowitz - HTT Consulng

Nik Teague – Verisign

Liang "Frank" Xia - Huawei

Introducción y contexto

draft-ietf-dots-use-cases-00 Resumen

- Proporciona ejemplos de casos de uso de DOTS (en realidad, categorías).
- Todos los ejemplos pueden ser CE/PE o PE/PE.
- Hay espacio para una amplia variación dentro de cada categoría (véase 4.1.1).
- Todas las comunicaciones DOTS de cada ejemplo pueden ser directamente entre los servidores DOTS y los clientes DOTS, o con la mediación de Relés DOTS.
- Los relés DOTS pueden reenviar mensajes entre clientes DOTS y los servidores que utilizan el transporte sin estado, el transporte con estado, o una combinación de ambos.
- Los relés DOTS pueden agregar solicitudes de servicio, estado mensajes y respuestas.
- Los relés DOTS pueden filtrar solicitudes de servicio, mensajes de estado y respuestas

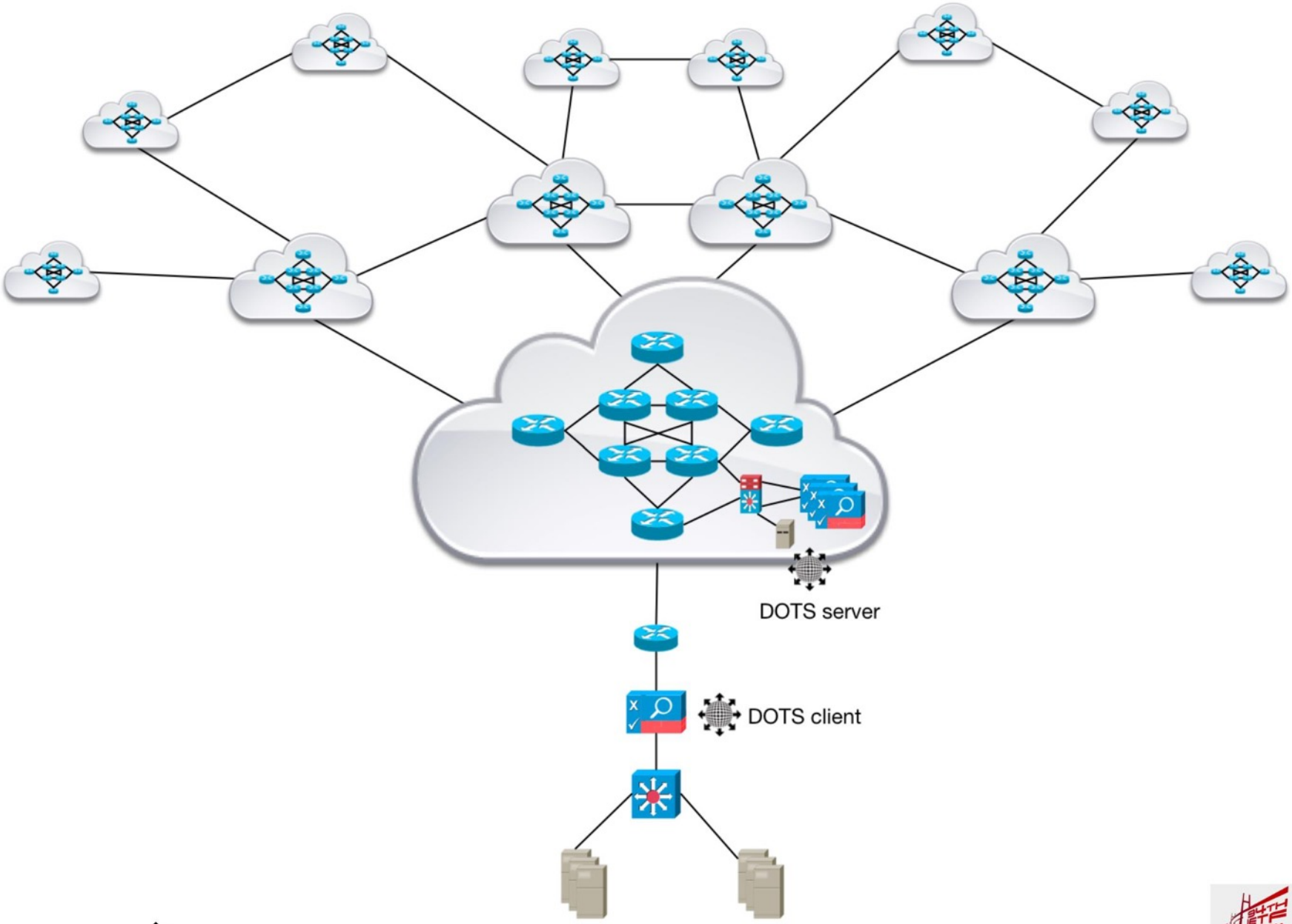
draft-ietf-dots-use-cases-00 Resumen (cont.)

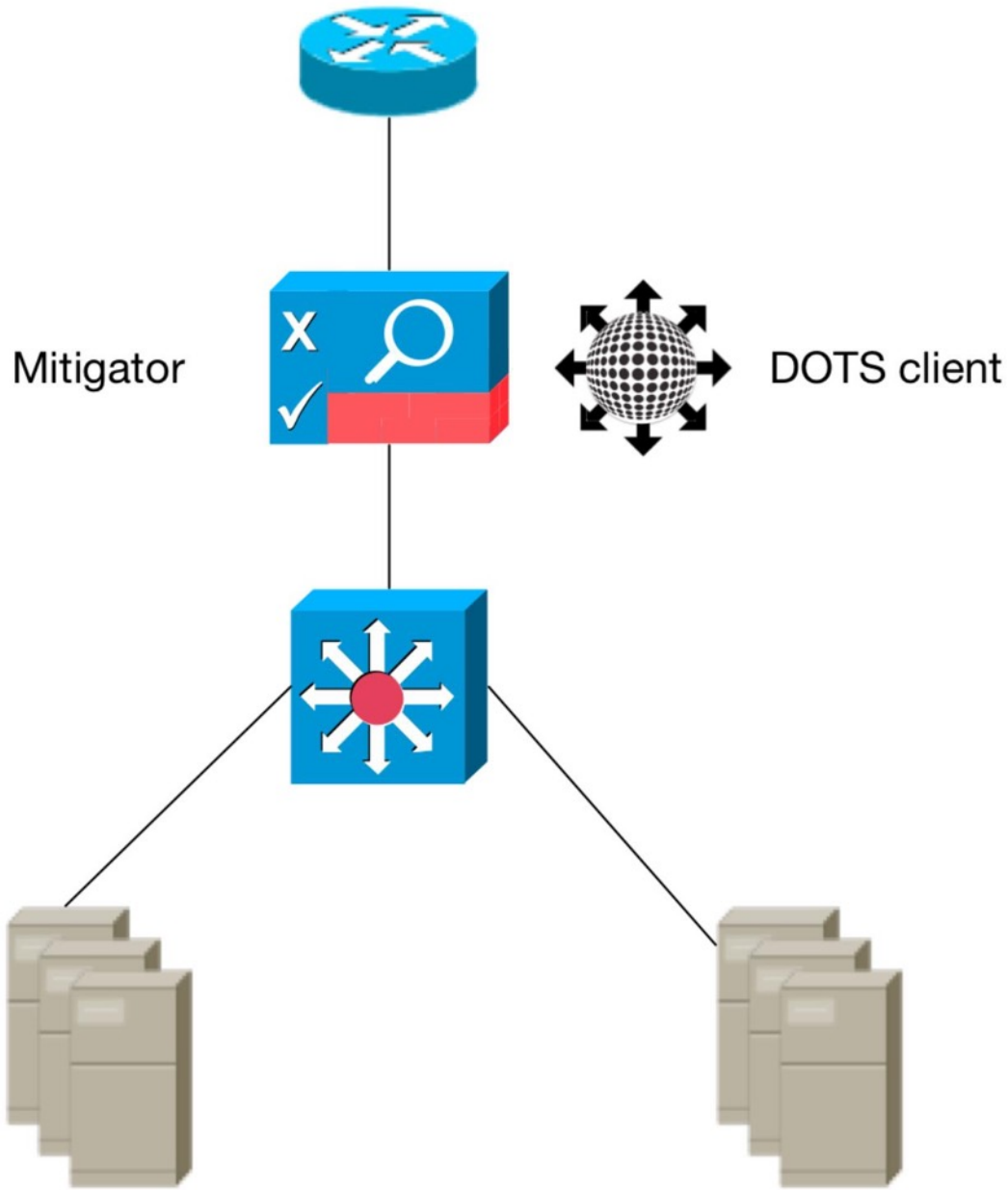
- Los casos de uso en -00 no son exhaustivos, son ilustrativos.
- Los casos de uso en -00 se centran en la mitigación de DDoS utilizando dispositivos de mitigación. S/RTBH, flowspec, OpenFlow, etc. pueden También se puede utilizar para aprovechar la infraestructura de la red para DDoS mitigación.
- 4.1.1 el caso de uso en esta presentación ilustra el DOTS completo ciclo de comunicaciones, variantes.
- Otros casos de uso en esta presentación son los "diffs" resumidos ilustrando el modelo de comunicación DOTS en una gran variedad de circunstancias.
- Los casos de uso de esta presentación se centran en la protección de los servidores bajo ataque DDoS en las redes de destino. DOTS también puede ser utilizado para suprimir el tráfico de ataque en las redes de origen o como atraviesa redes intermedias.

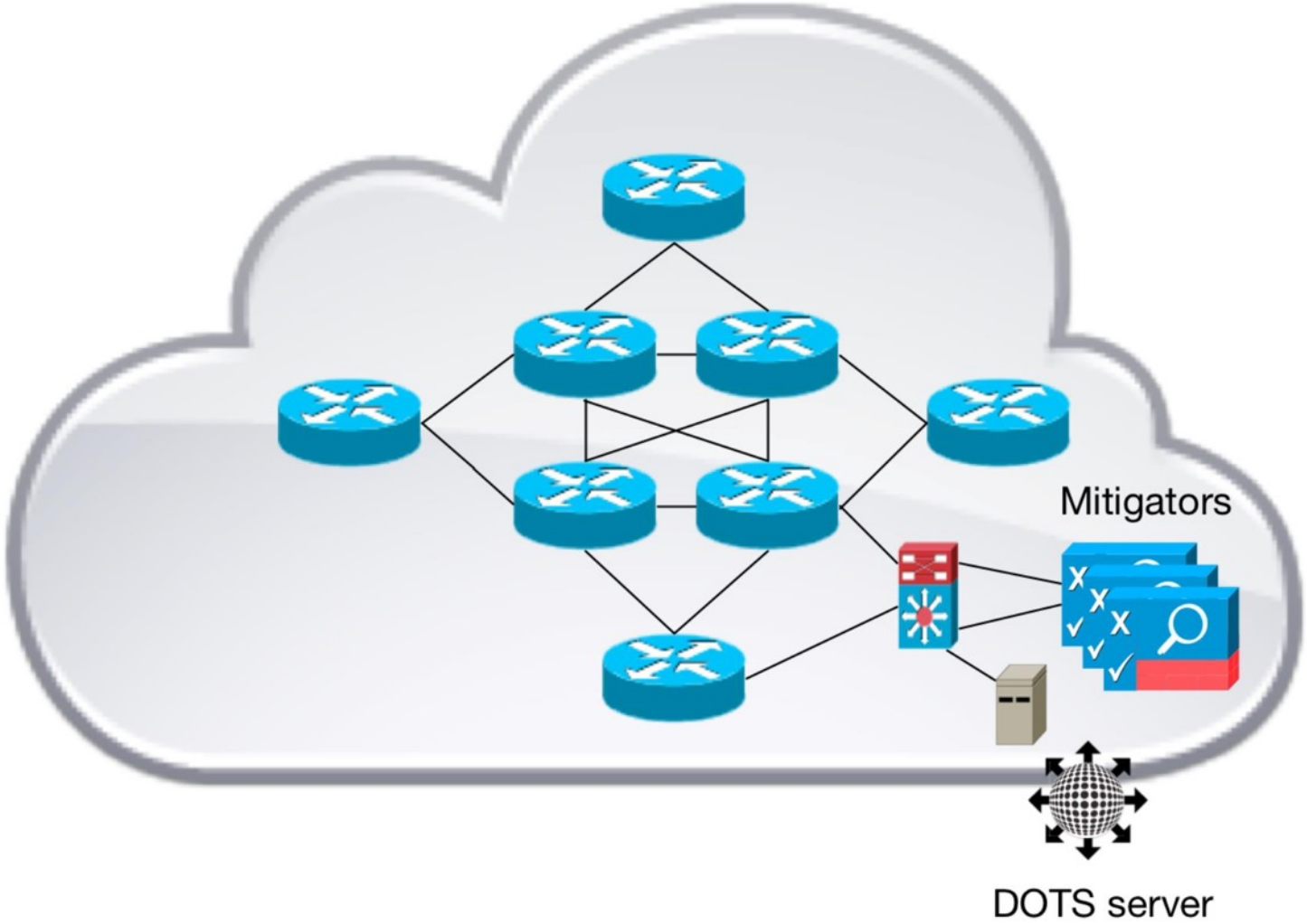
4.1 - Casos de uso principales

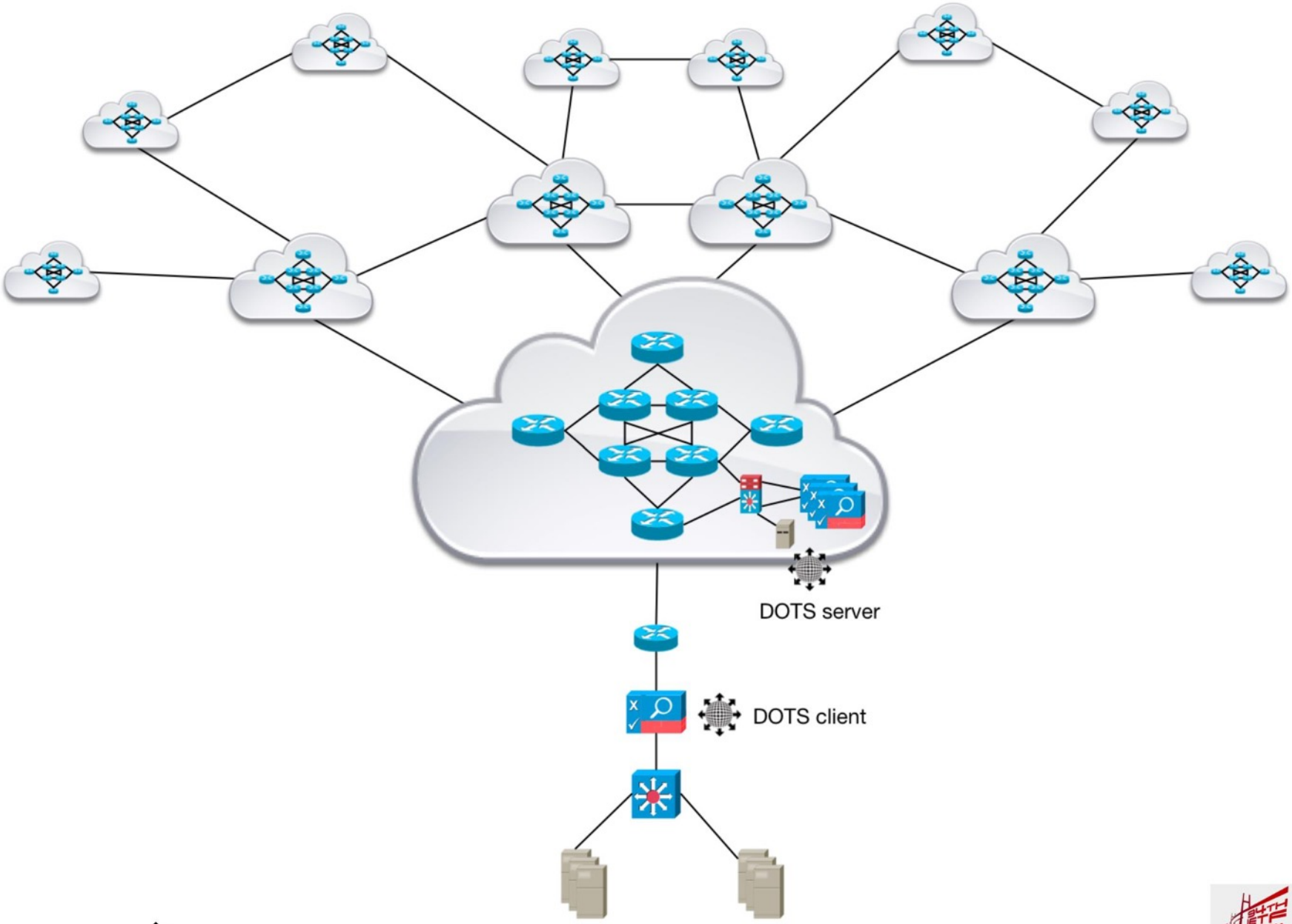
4.1.1 - Solicitud de mitigadores de CPE o PE

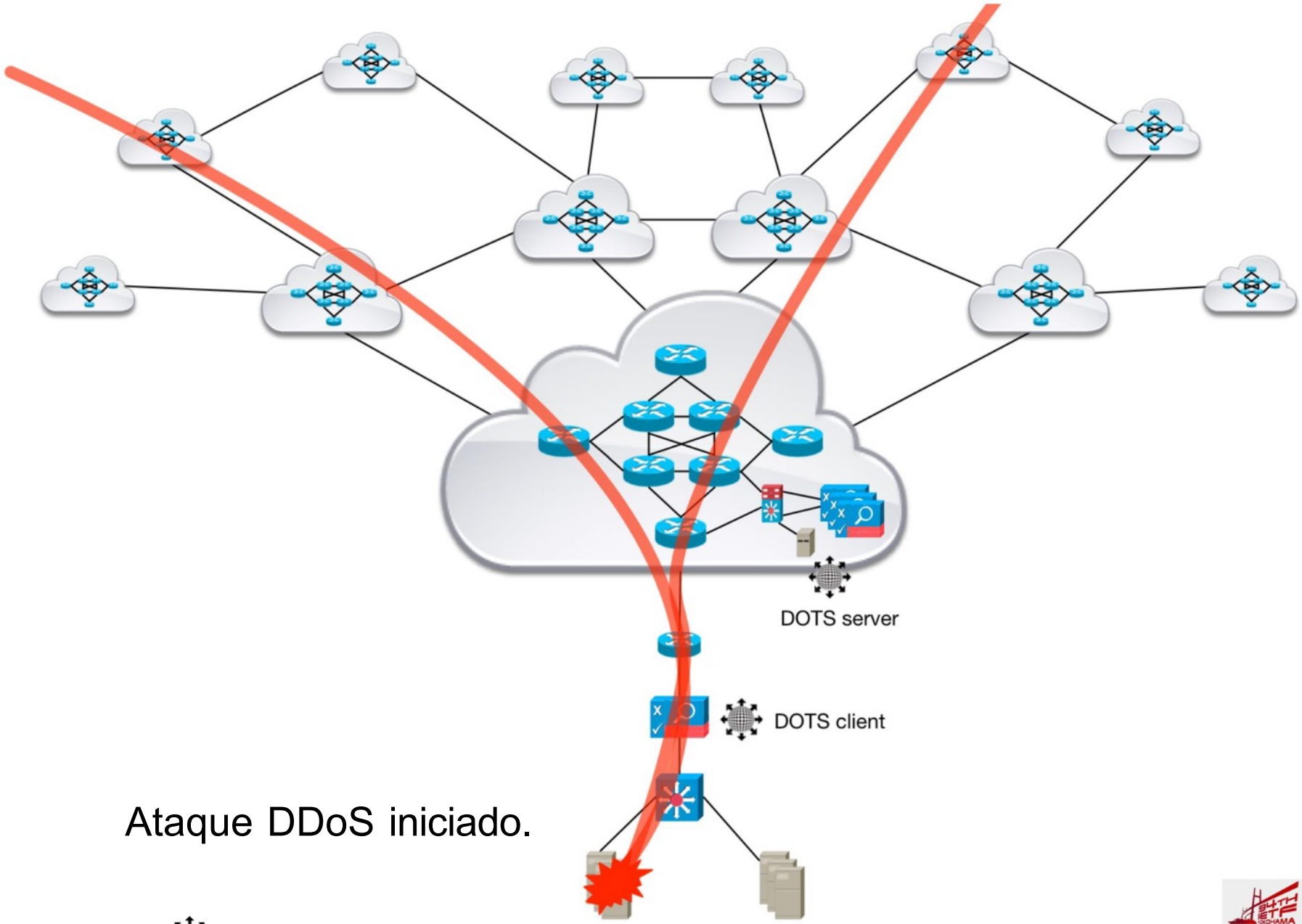
Mitigación de DDoS en sentido ascendent


DOTS server
DOTS client

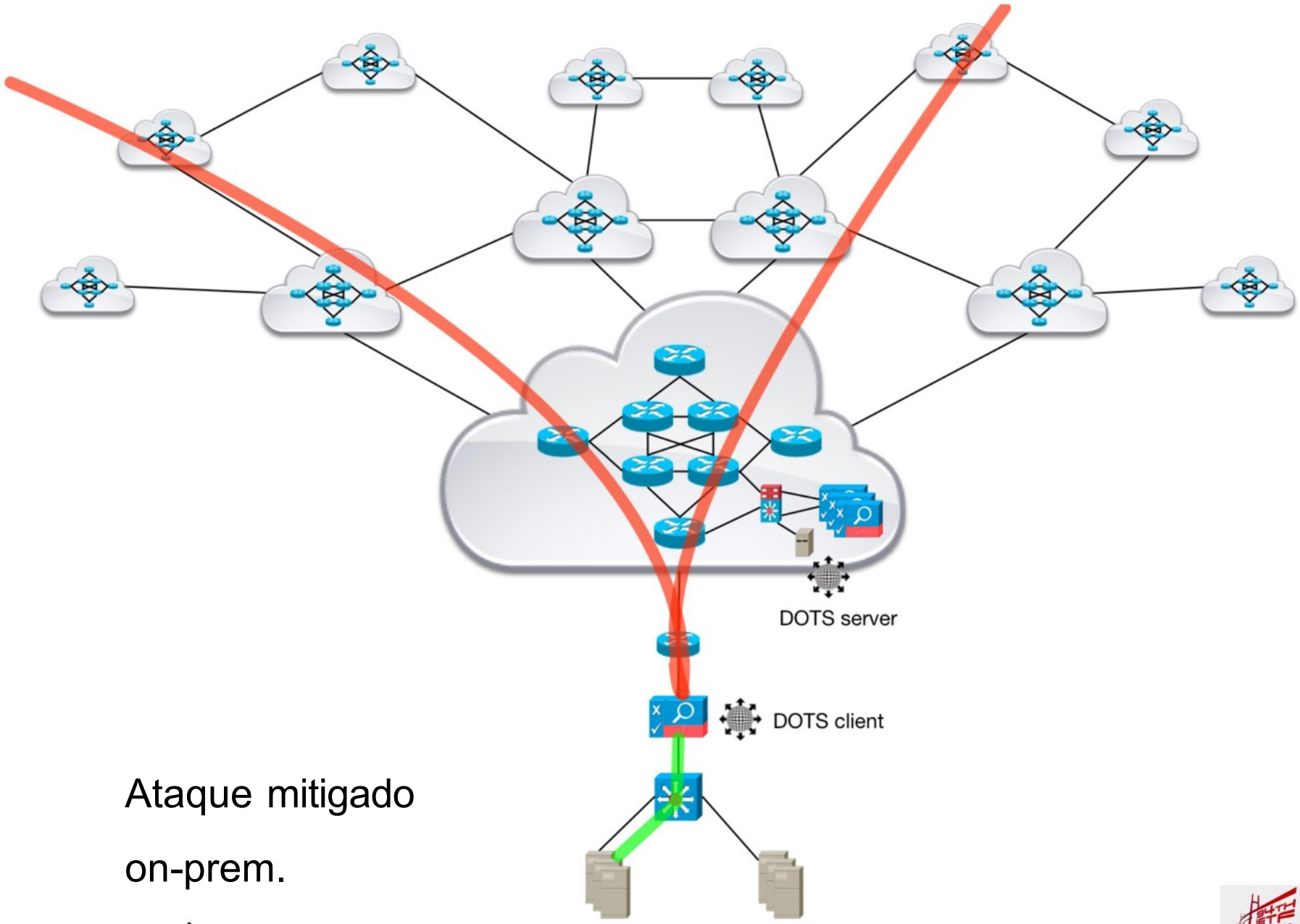

Mitigator
DOTS client


Mitigators
DOTS server


DOTS server
DOTS client

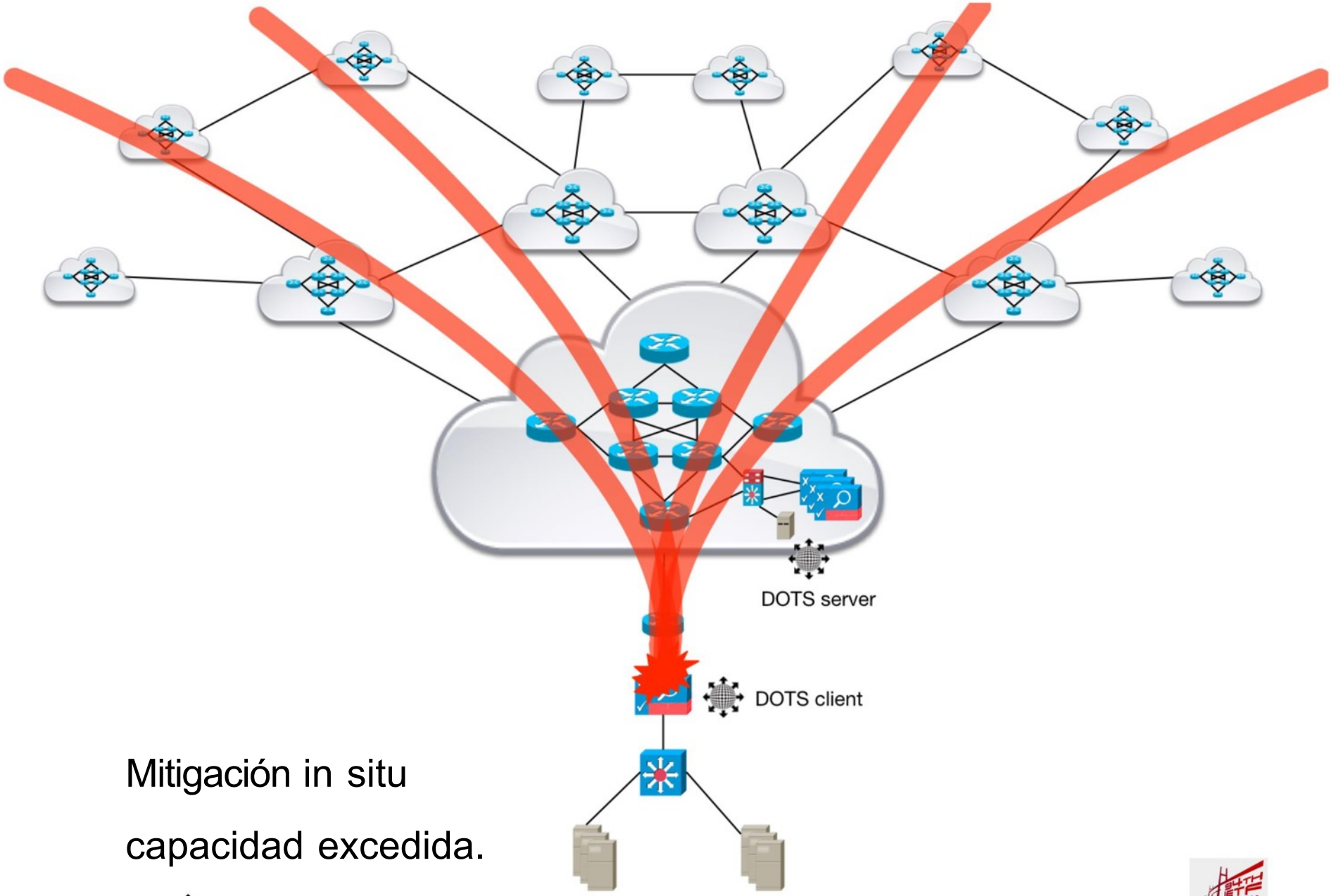


Ataque DDoS iniciado.



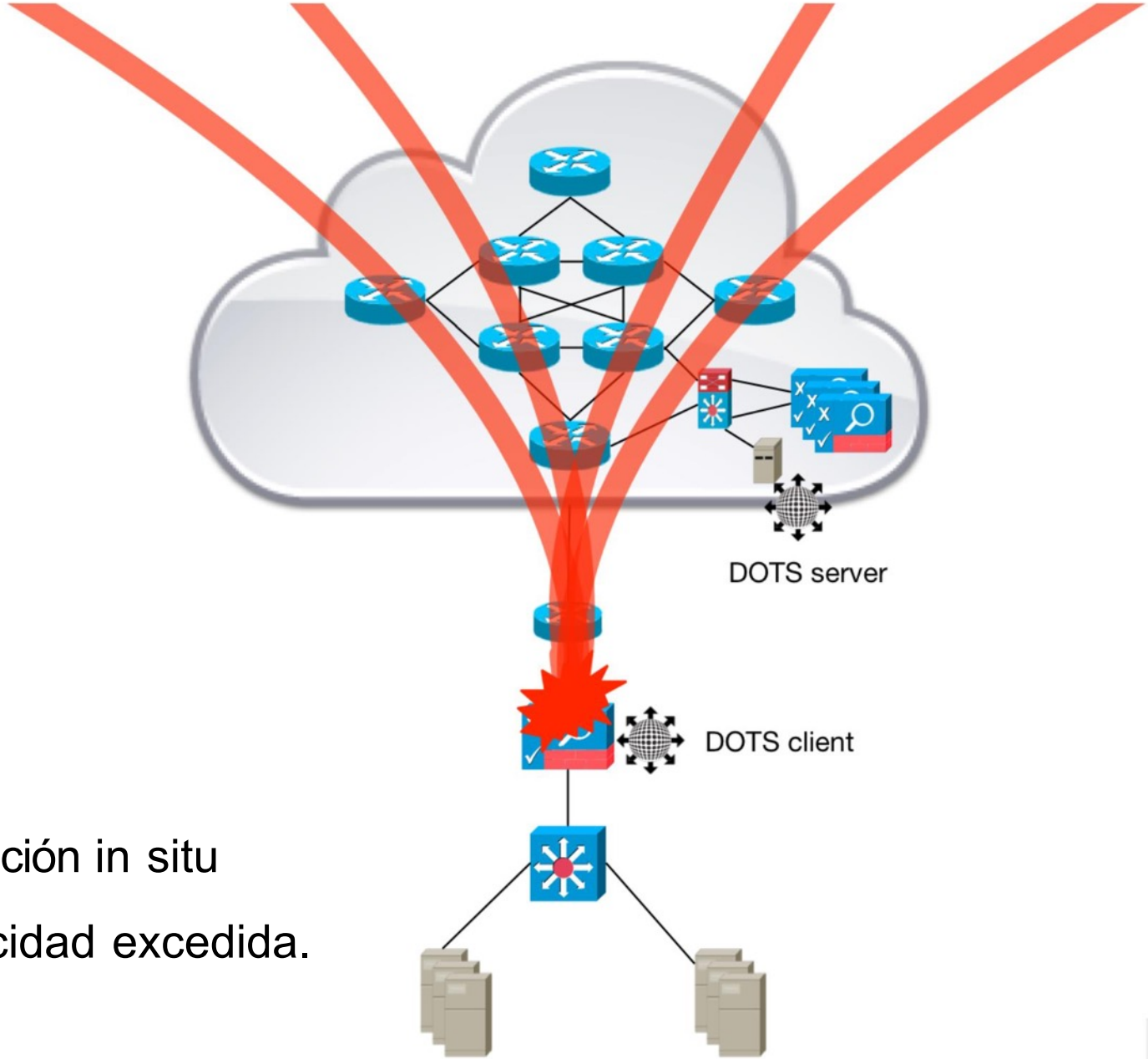
Ataque mitigado

on-prem.



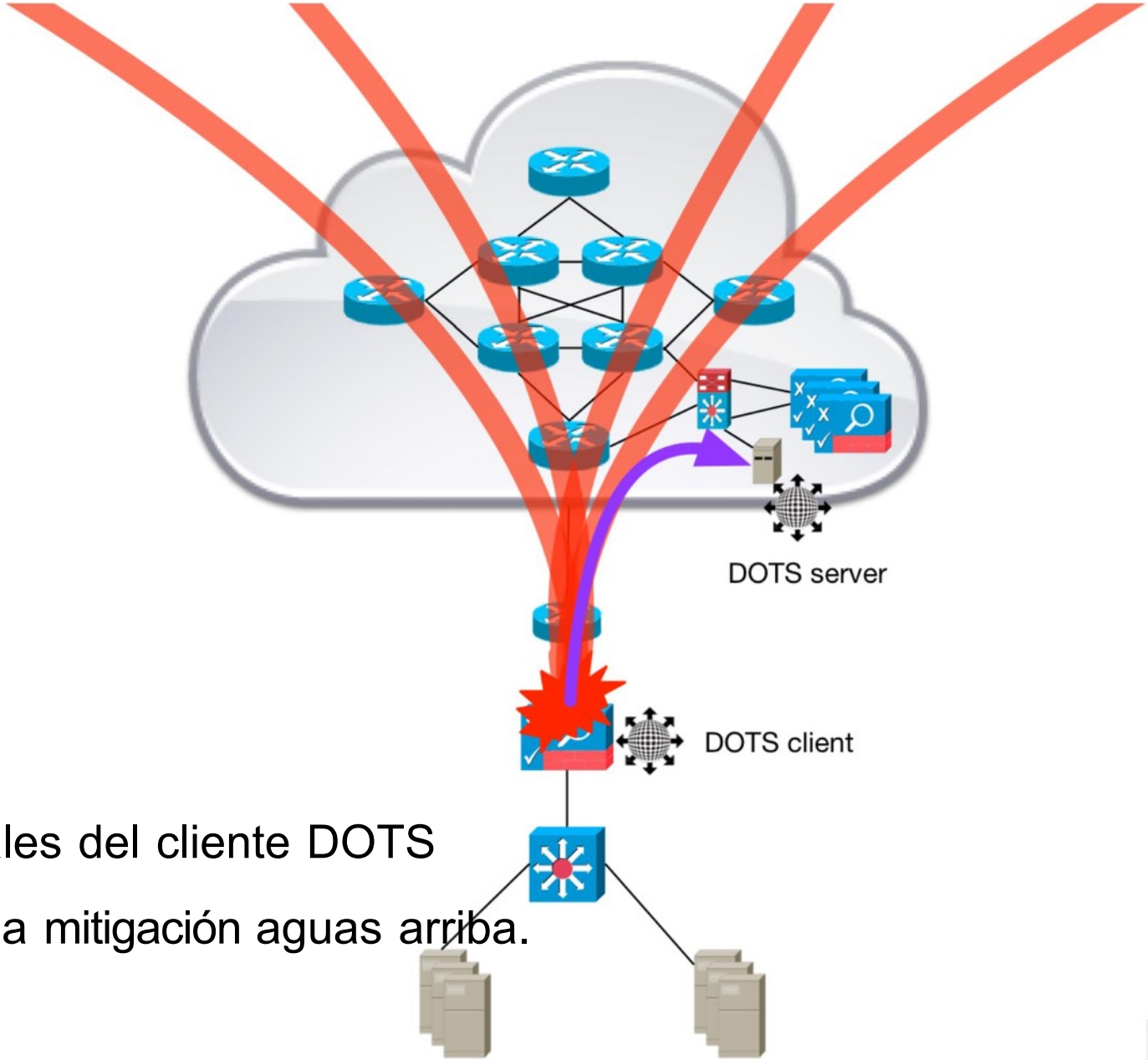
Mitigación in situ

capacidad excedida.



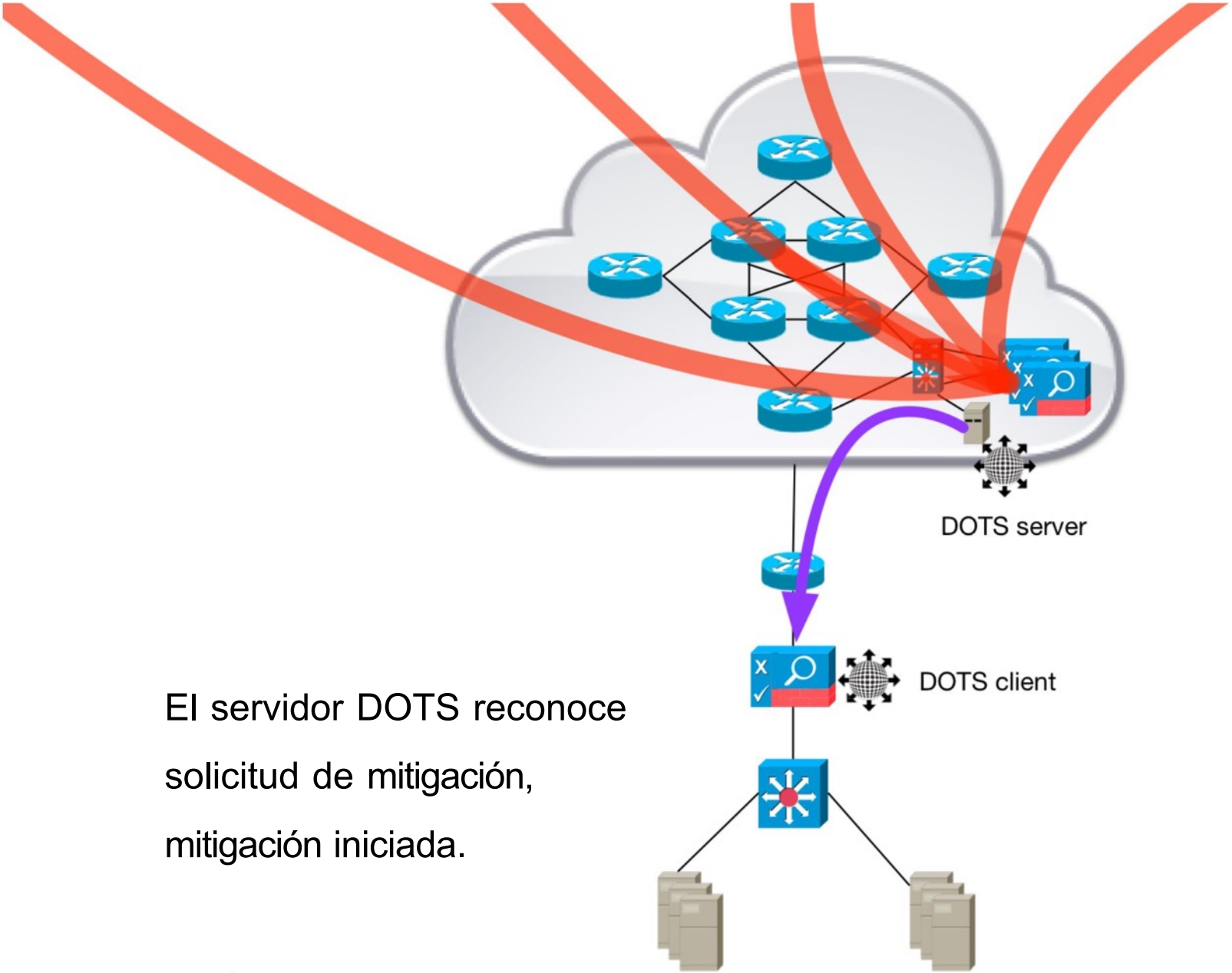
Mitigación in situ

capacidad excedida.

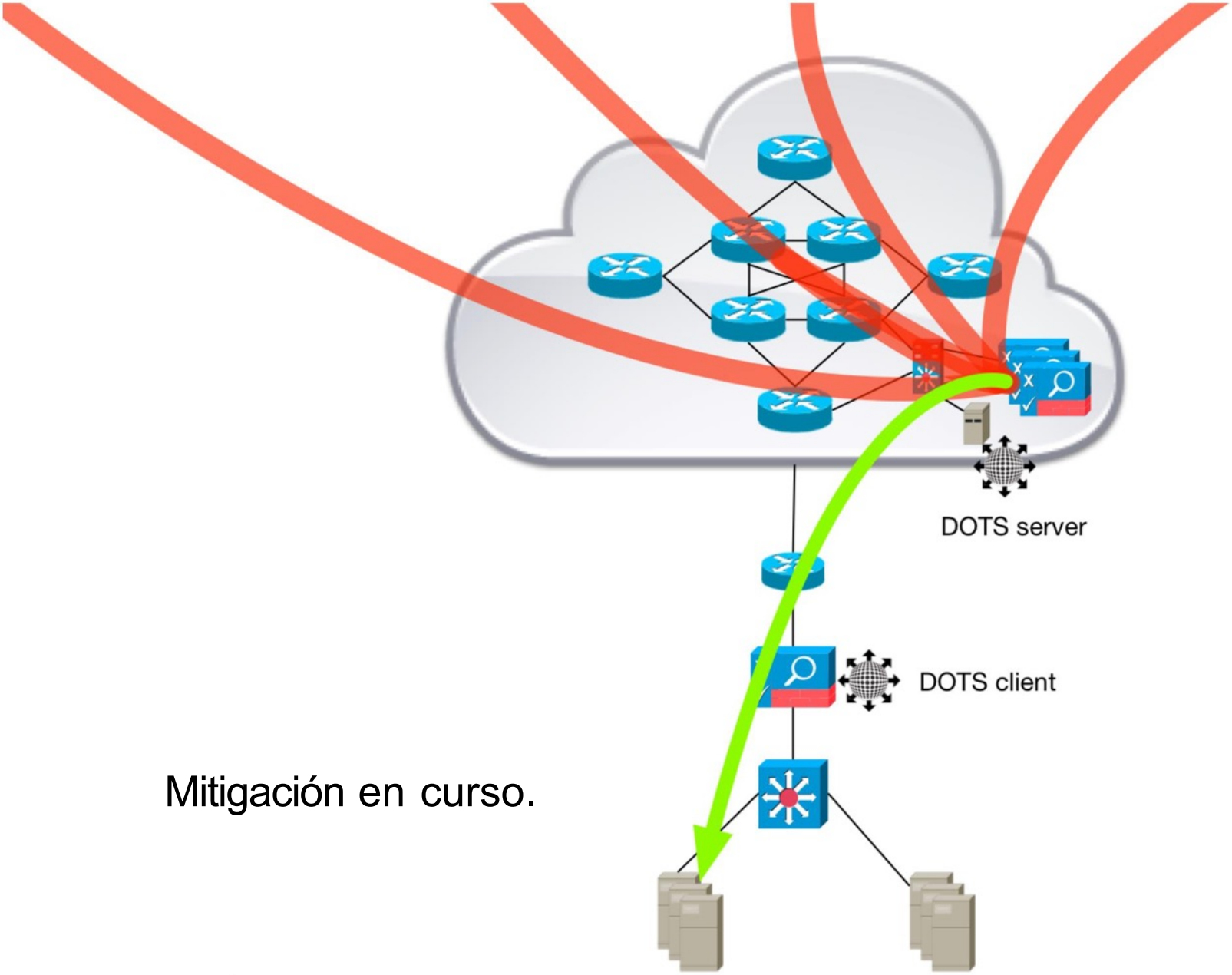


Señales del cliente DOTS

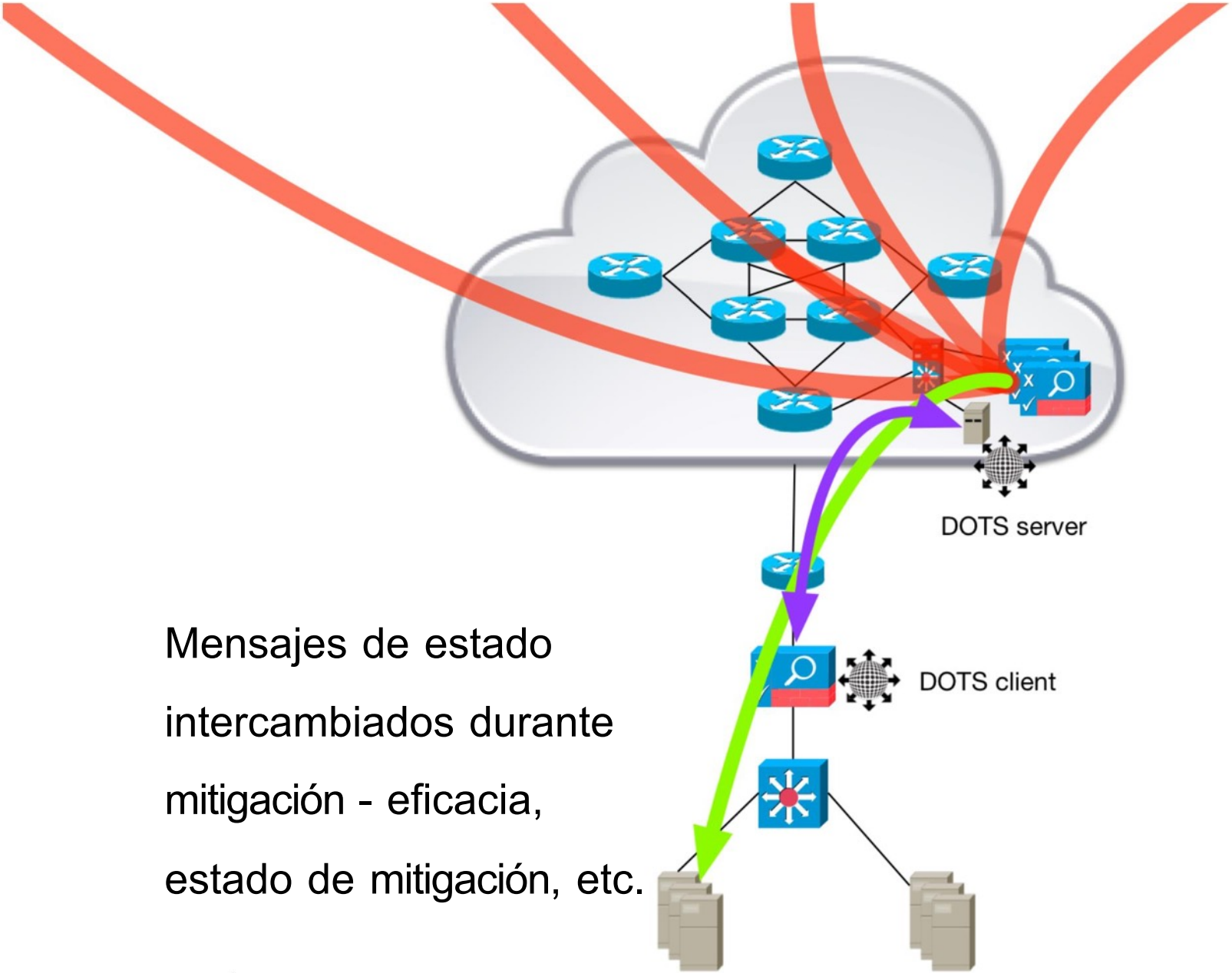
para la mitigación aguas arriba.



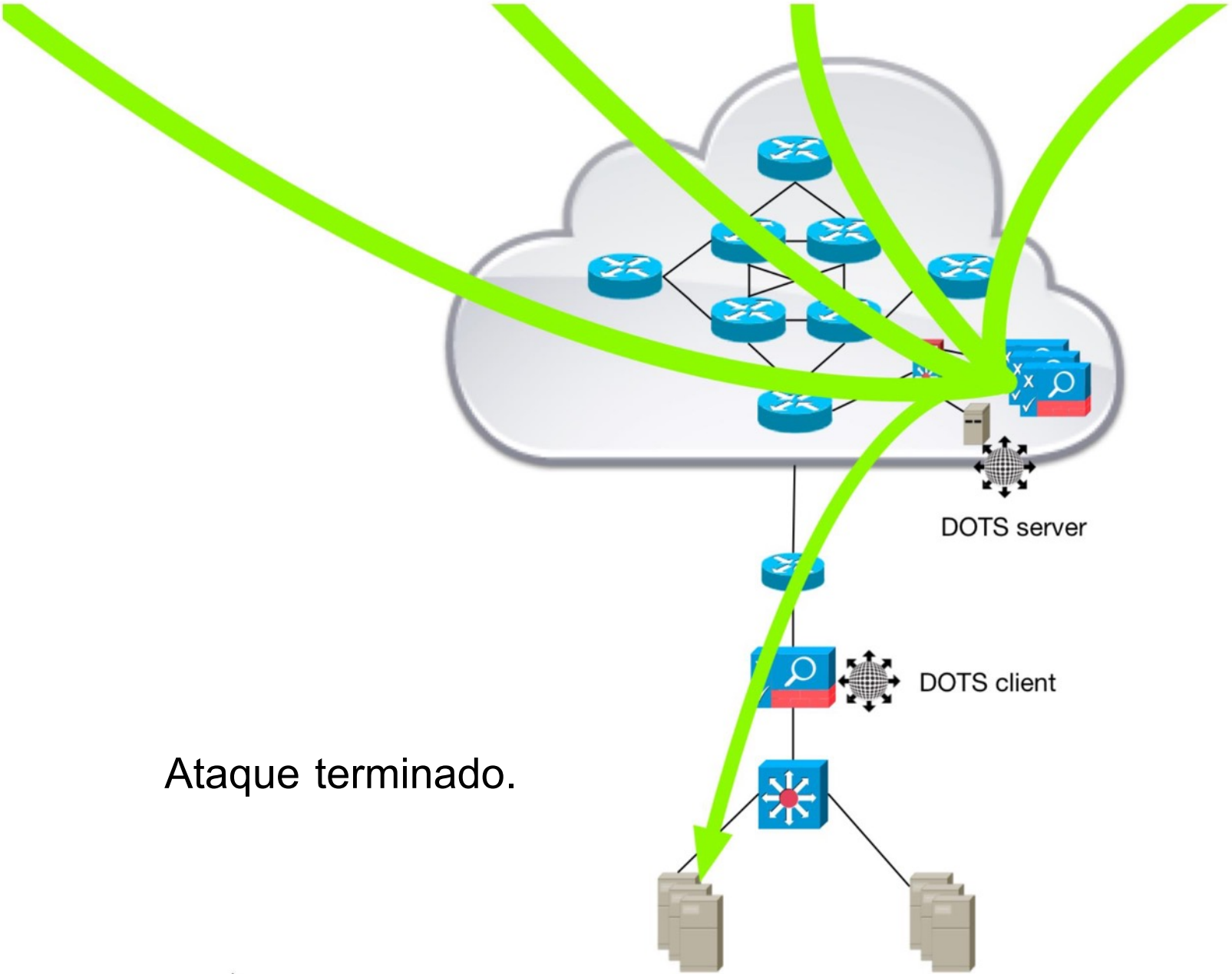
El servidor DOTS reconoce solicitud de mitigación, mitigación iniciada.



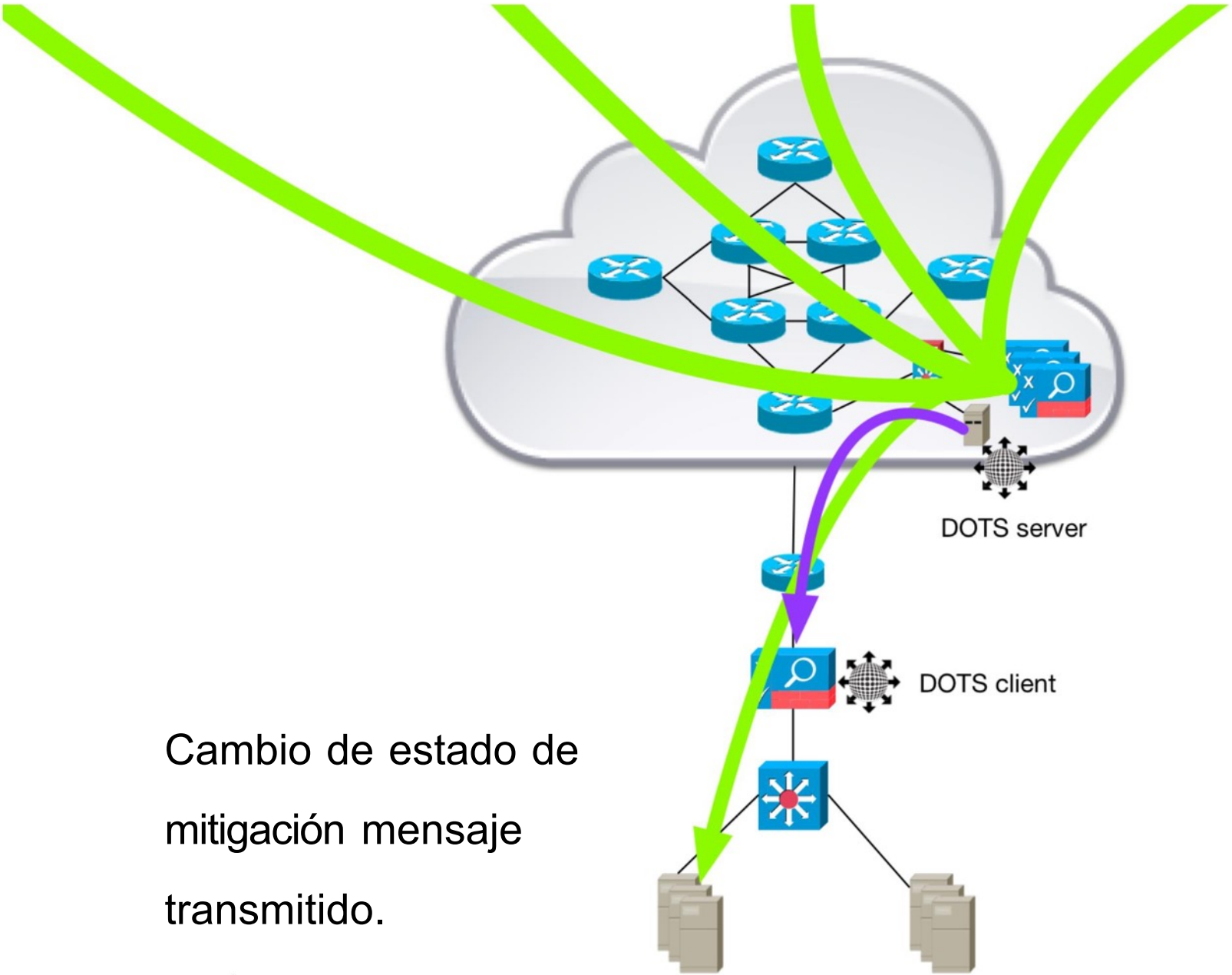
Mitigación en curso.



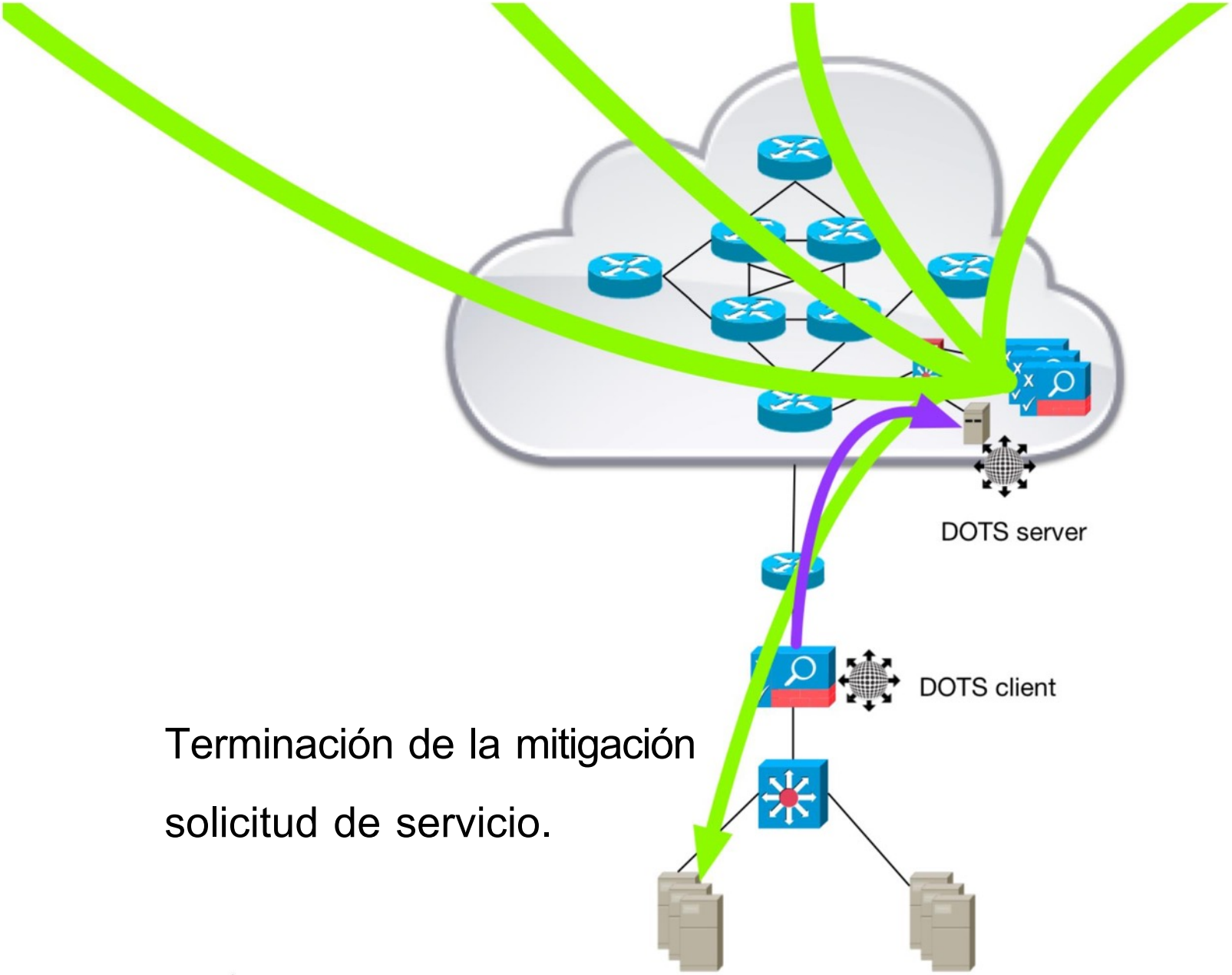
Mensajes de estado intercambiados durante mitigación - eficacia, estado de mitigación, etc.



Ataque terminado.

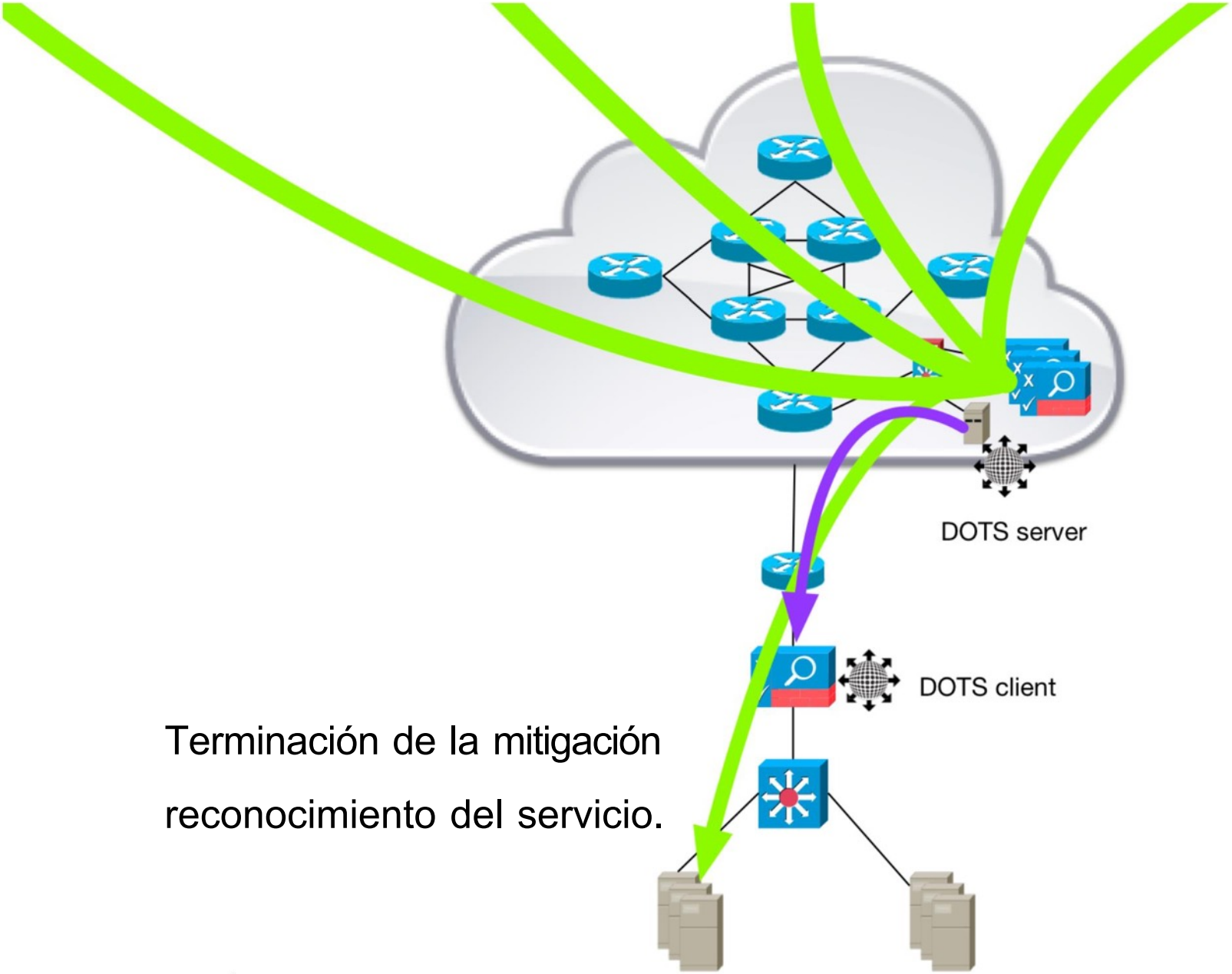


Cambio de estado de mitigación mensaje transmitido.



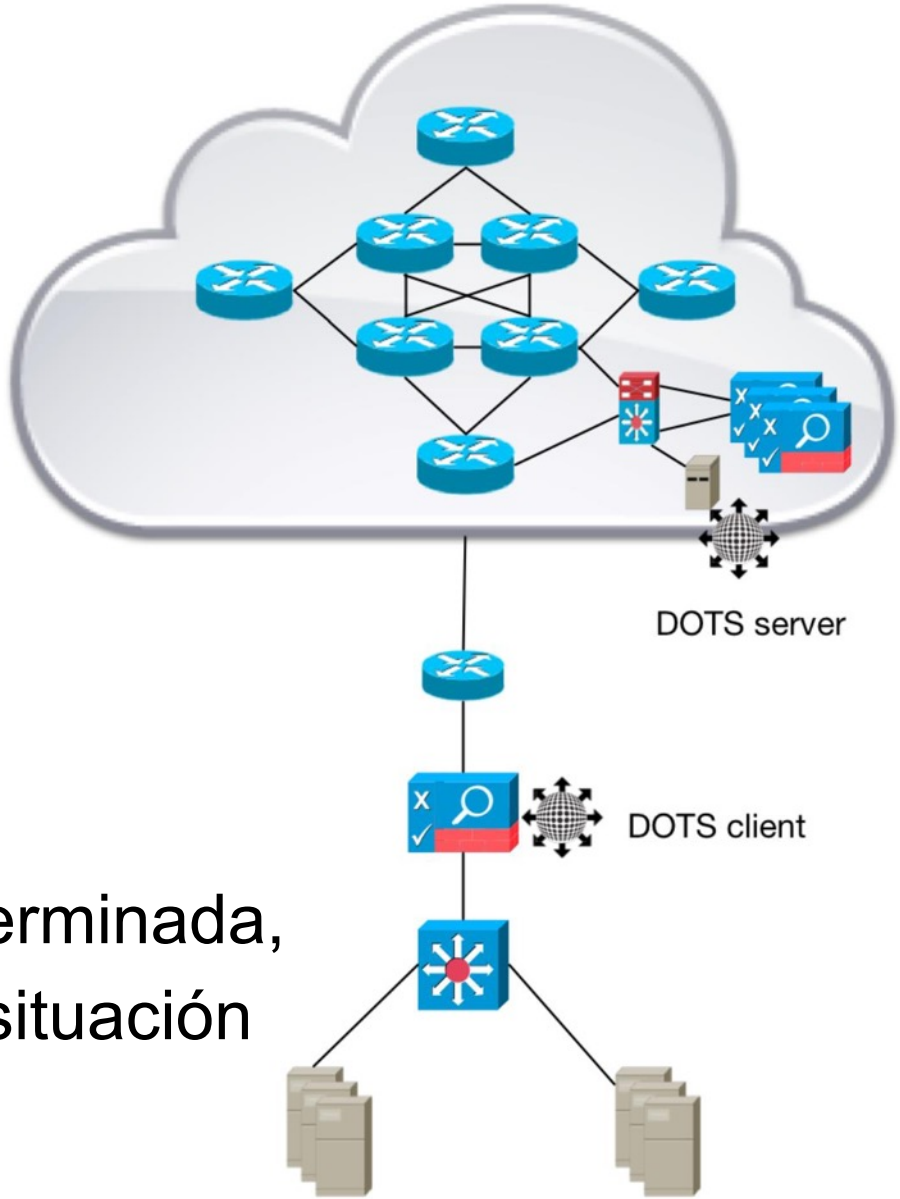
Terminación de la mitigación

solicitud de servicio.



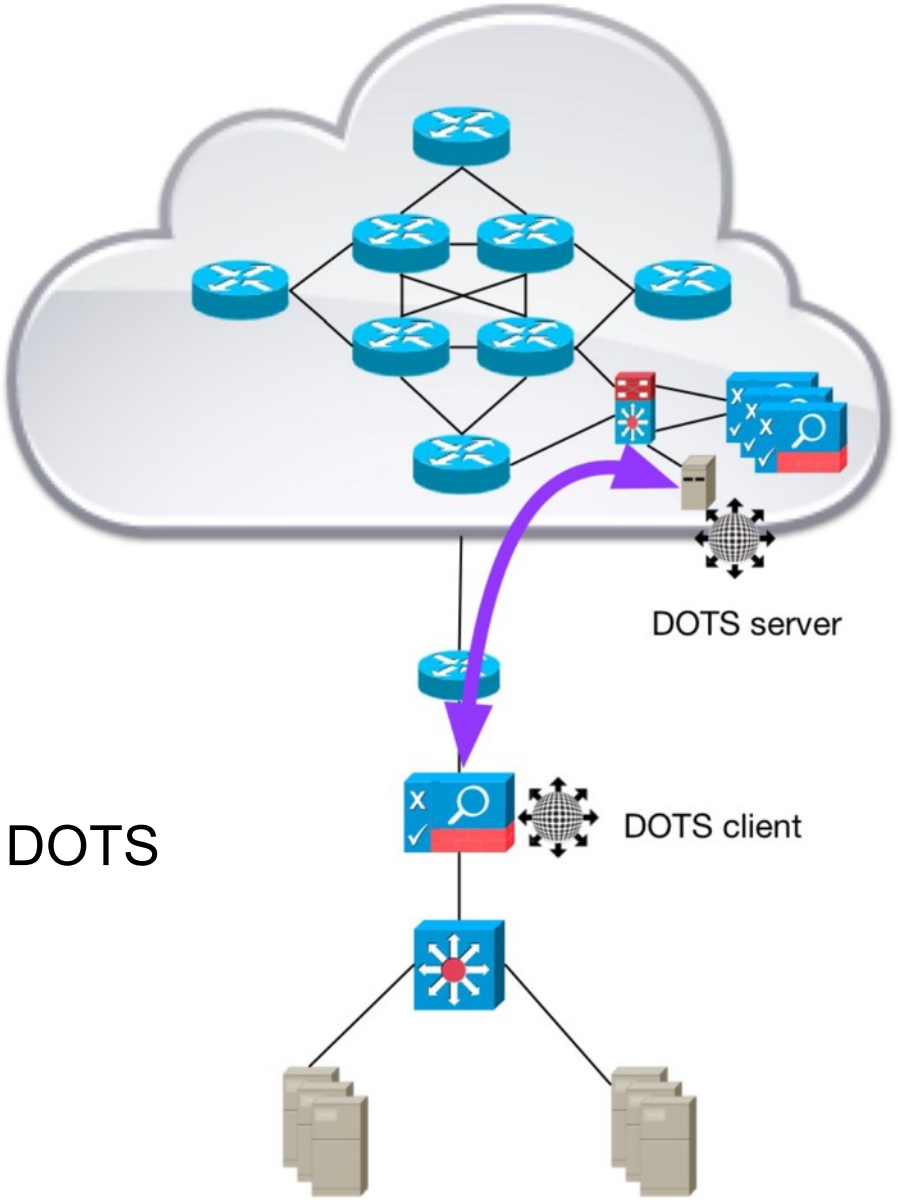
Terminación de la mitigación

reconocimiento del servicio.



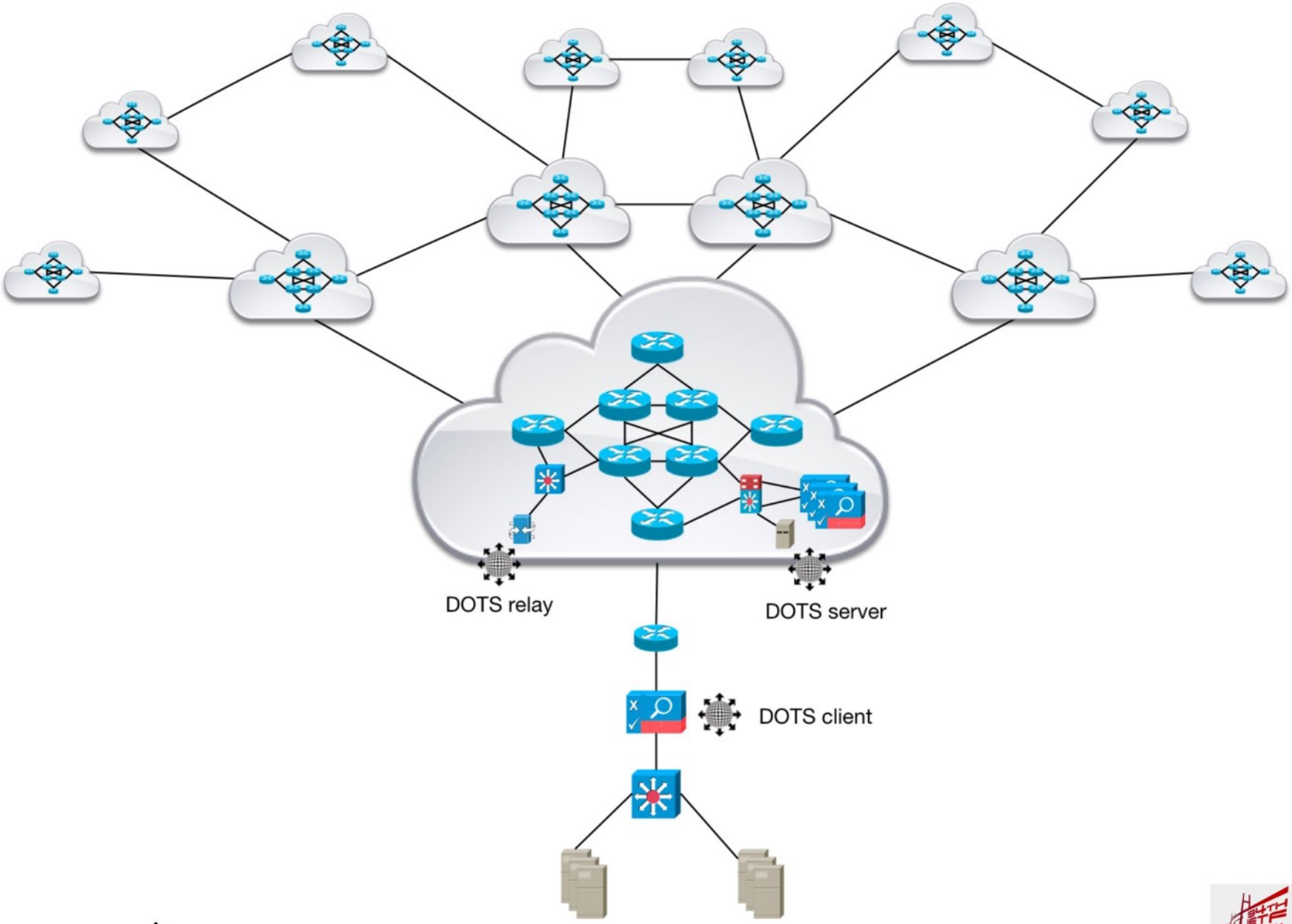
Mitigación terminada, volver a la situación anterior.

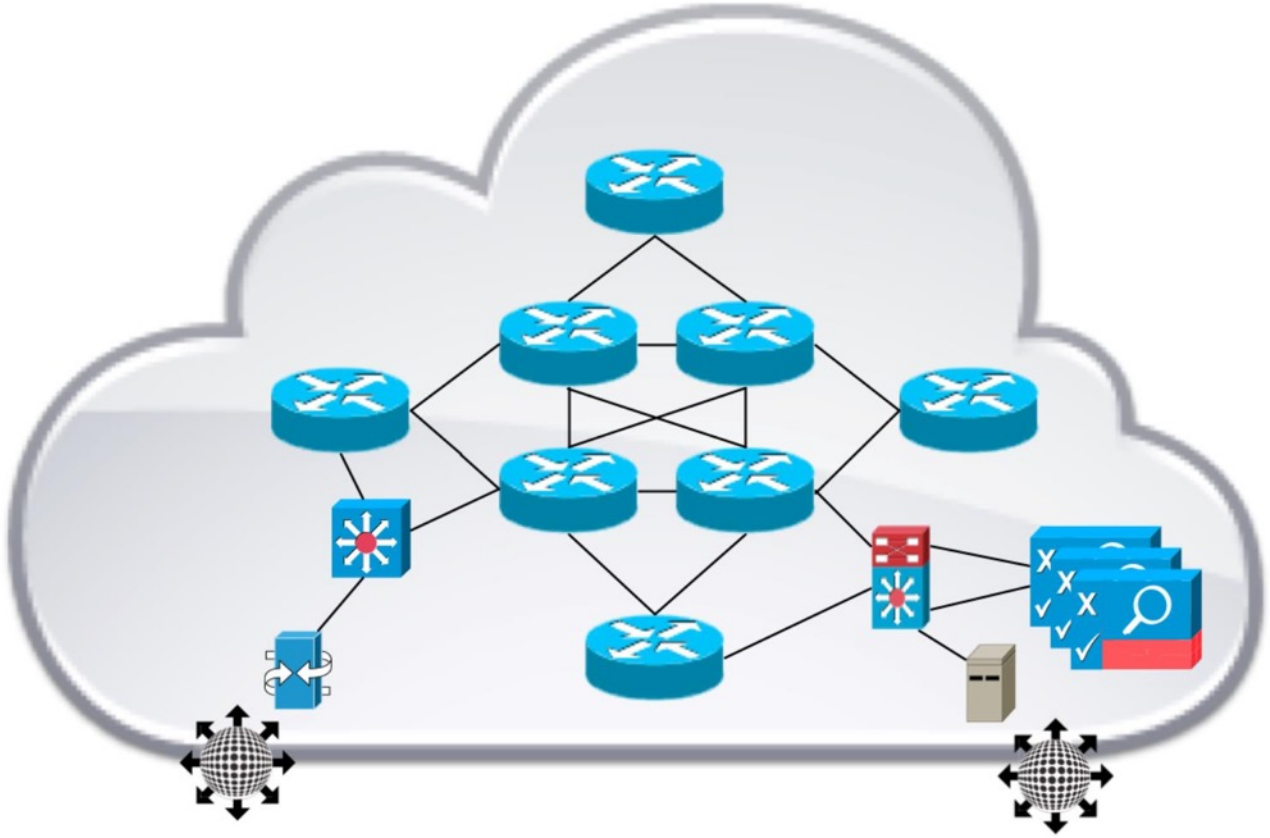
Comunicación DOTS relaciones.

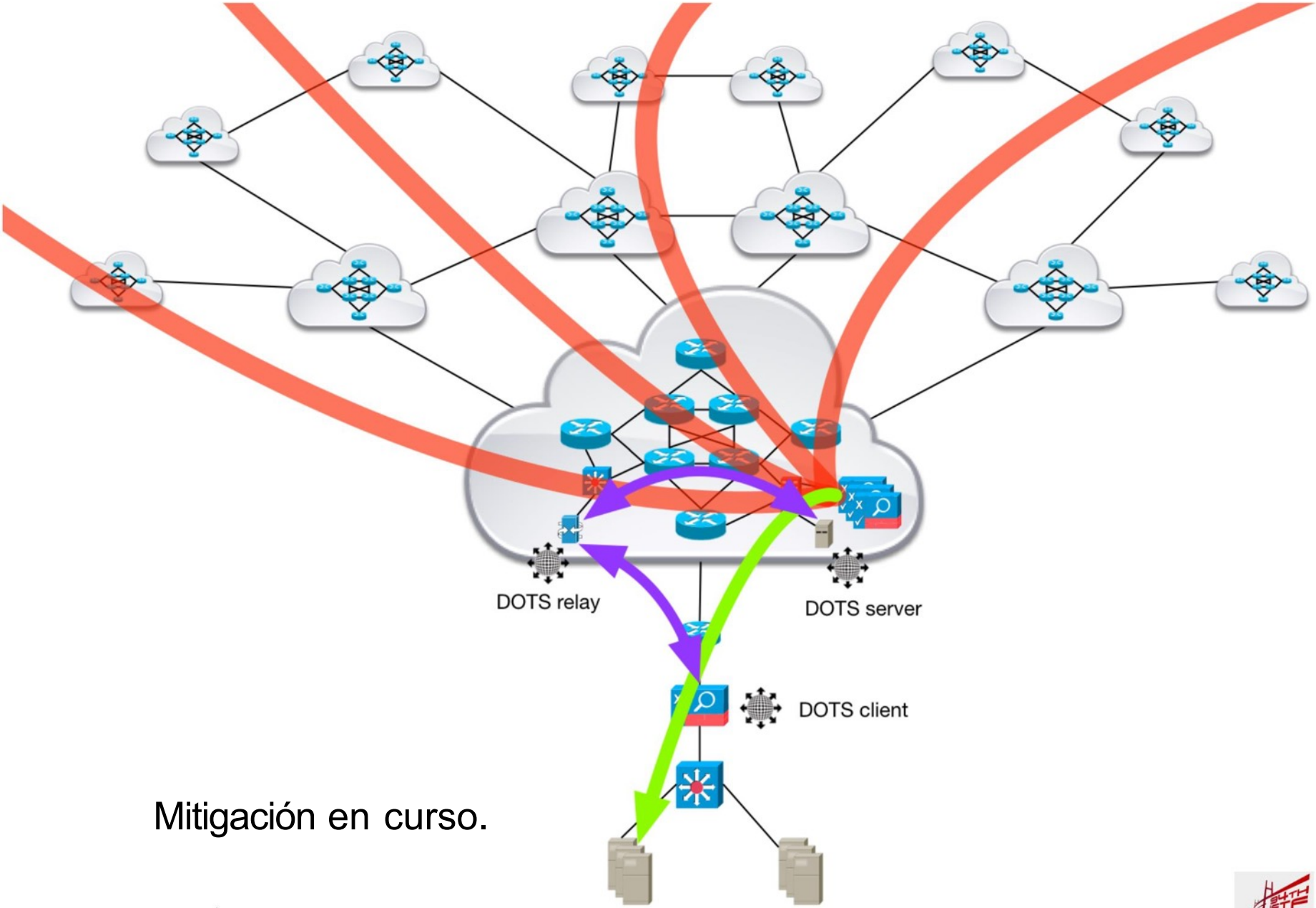


4.1.1 - Variación con el relé DOTS

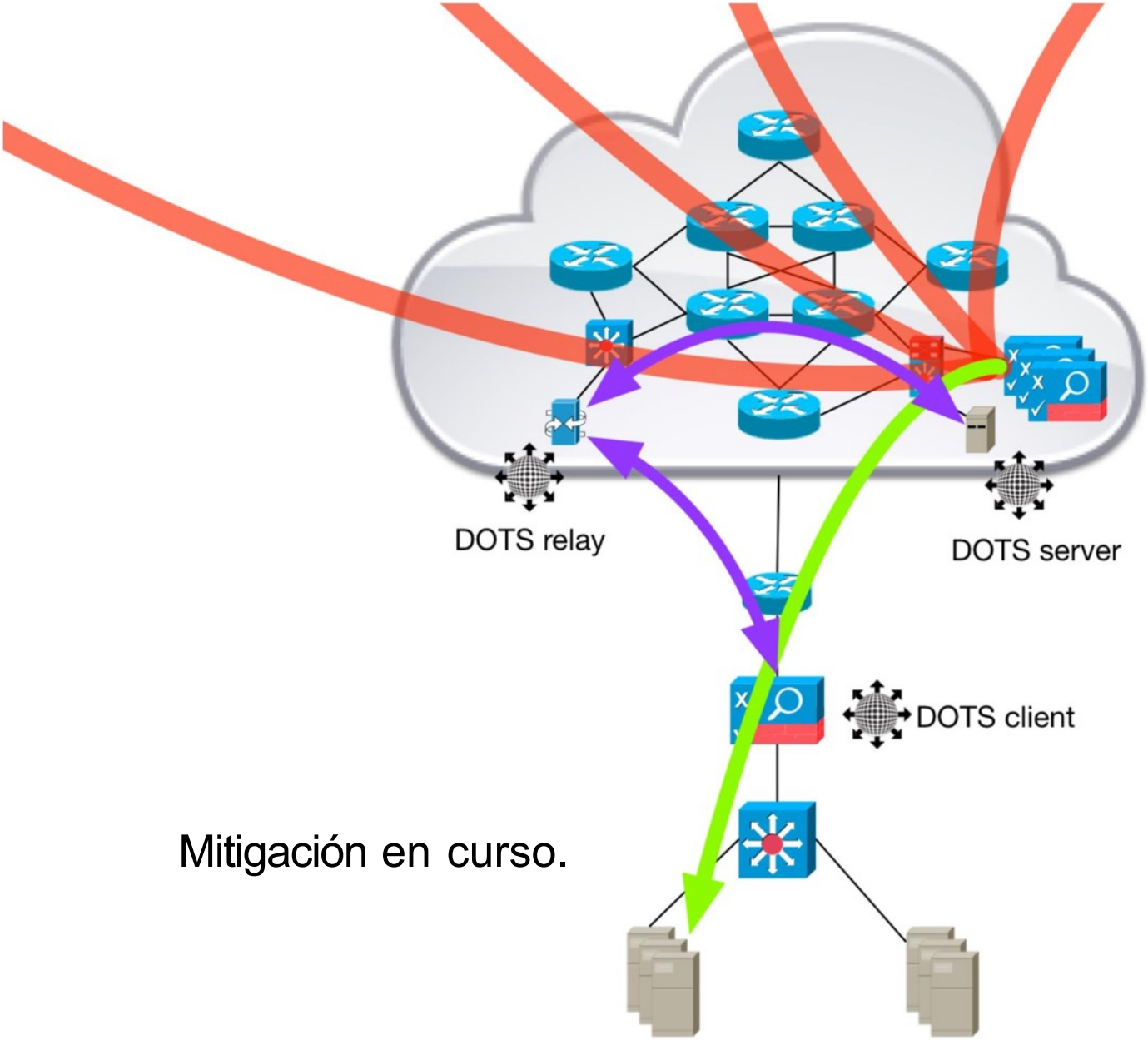
Comunicaciones


DOTS relay
DOTS server
DOTS client

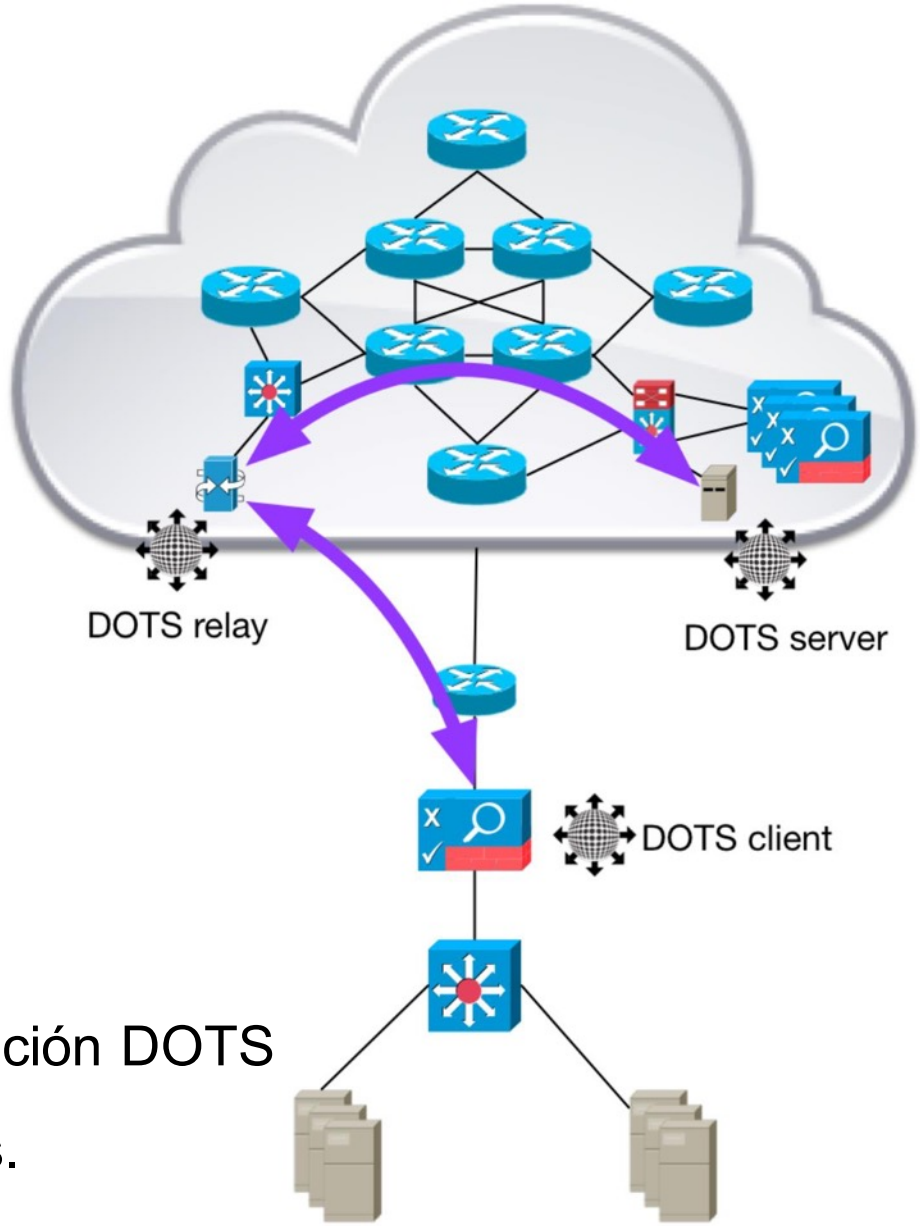

DOTS relay
DOTS server



Mitigación en curso.



Mitigación en curso.

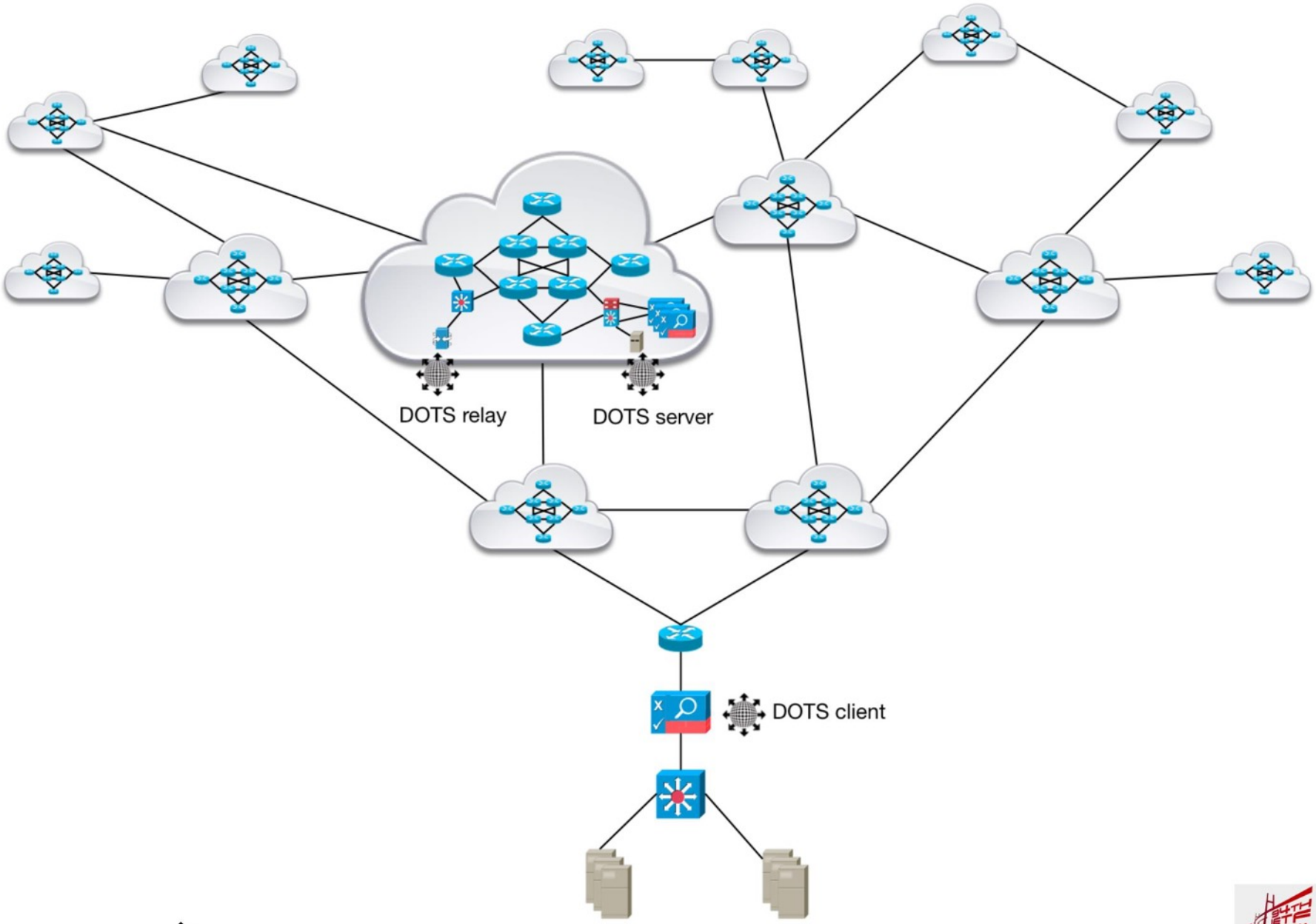


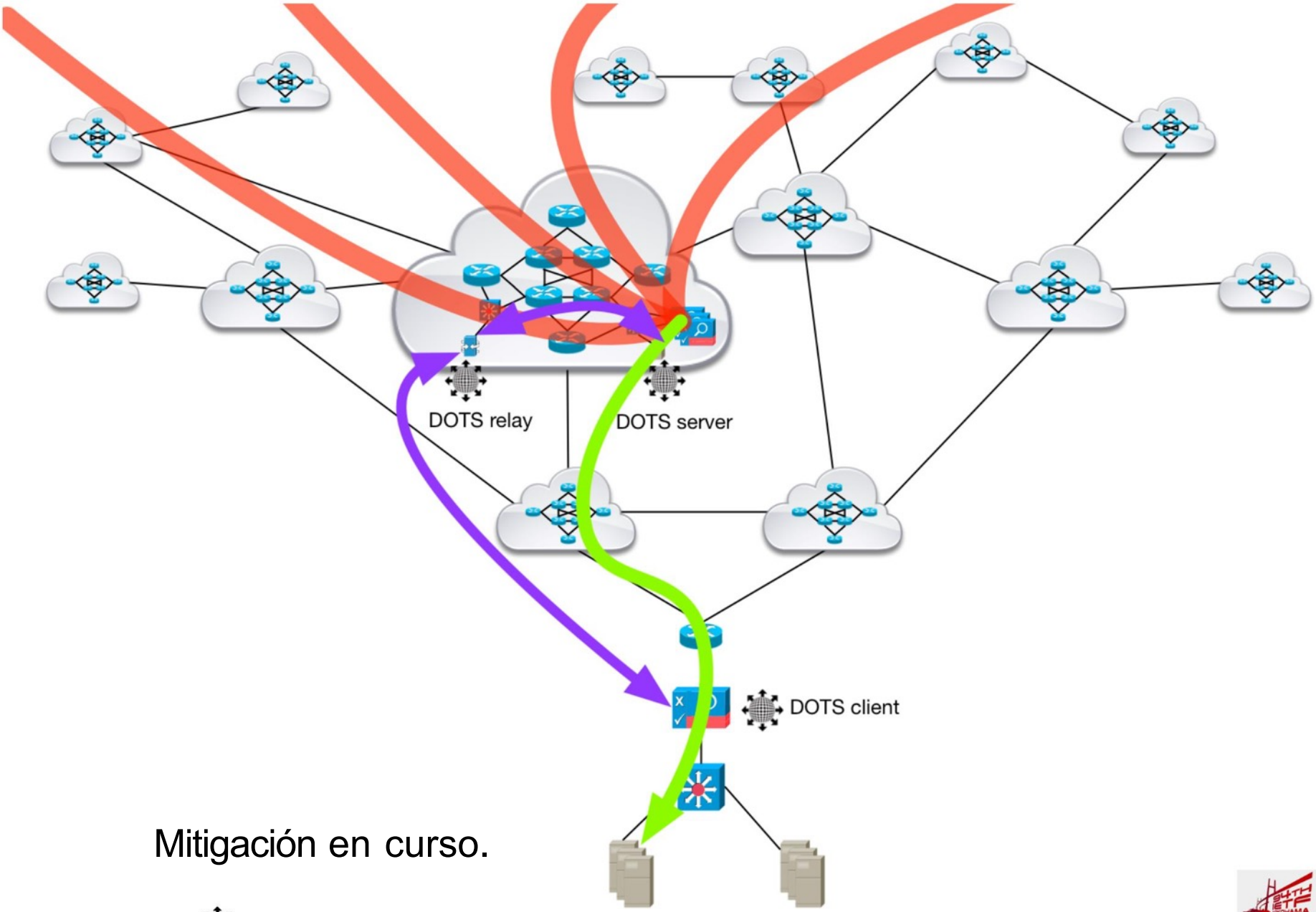
Comunicación DOTS

relaciones.

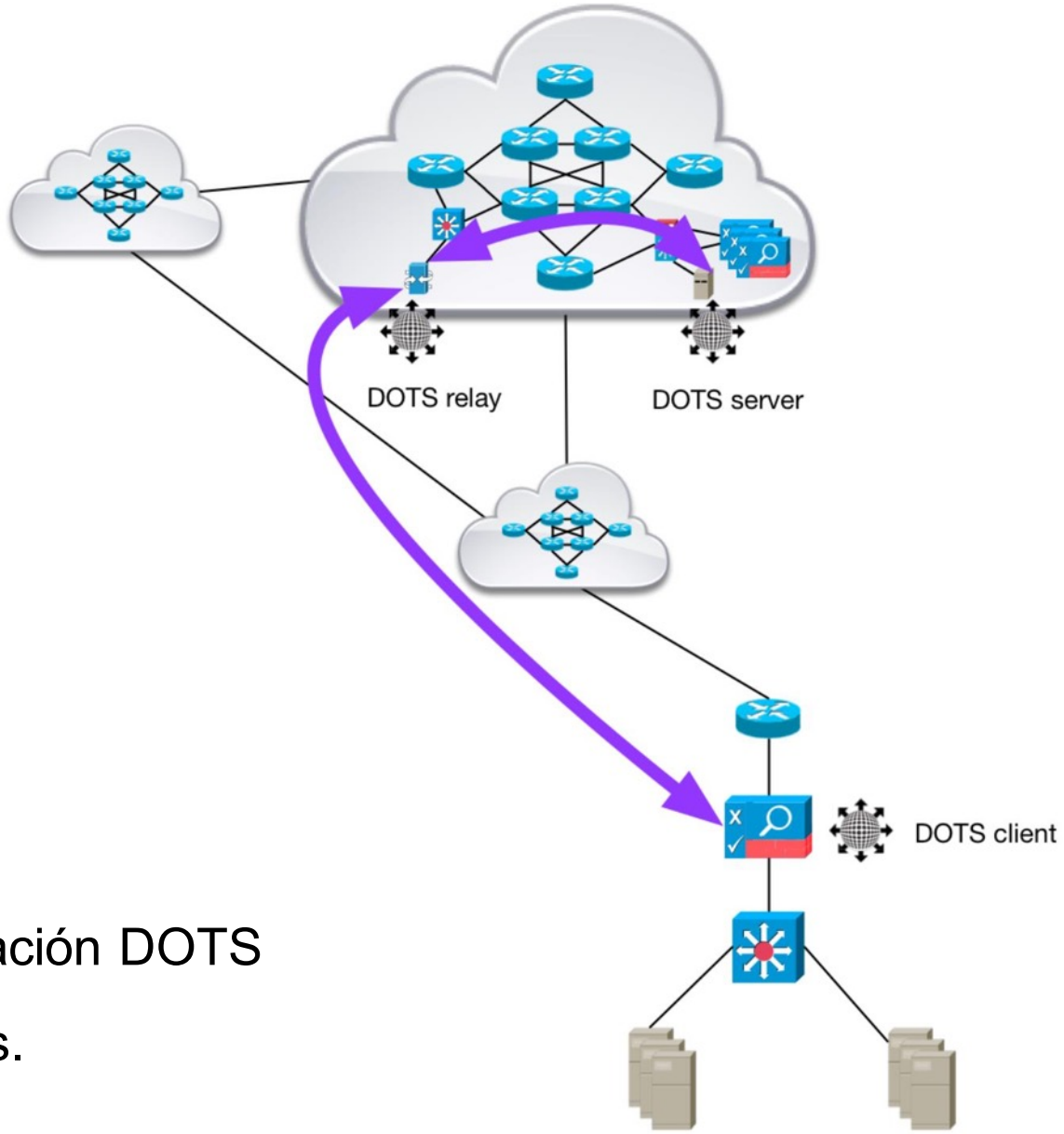
4.1.1 - Variación con DDoS superpuesto

Proveedor de servicios de mitigación


DOTS relay
DOTS server
DOTS client



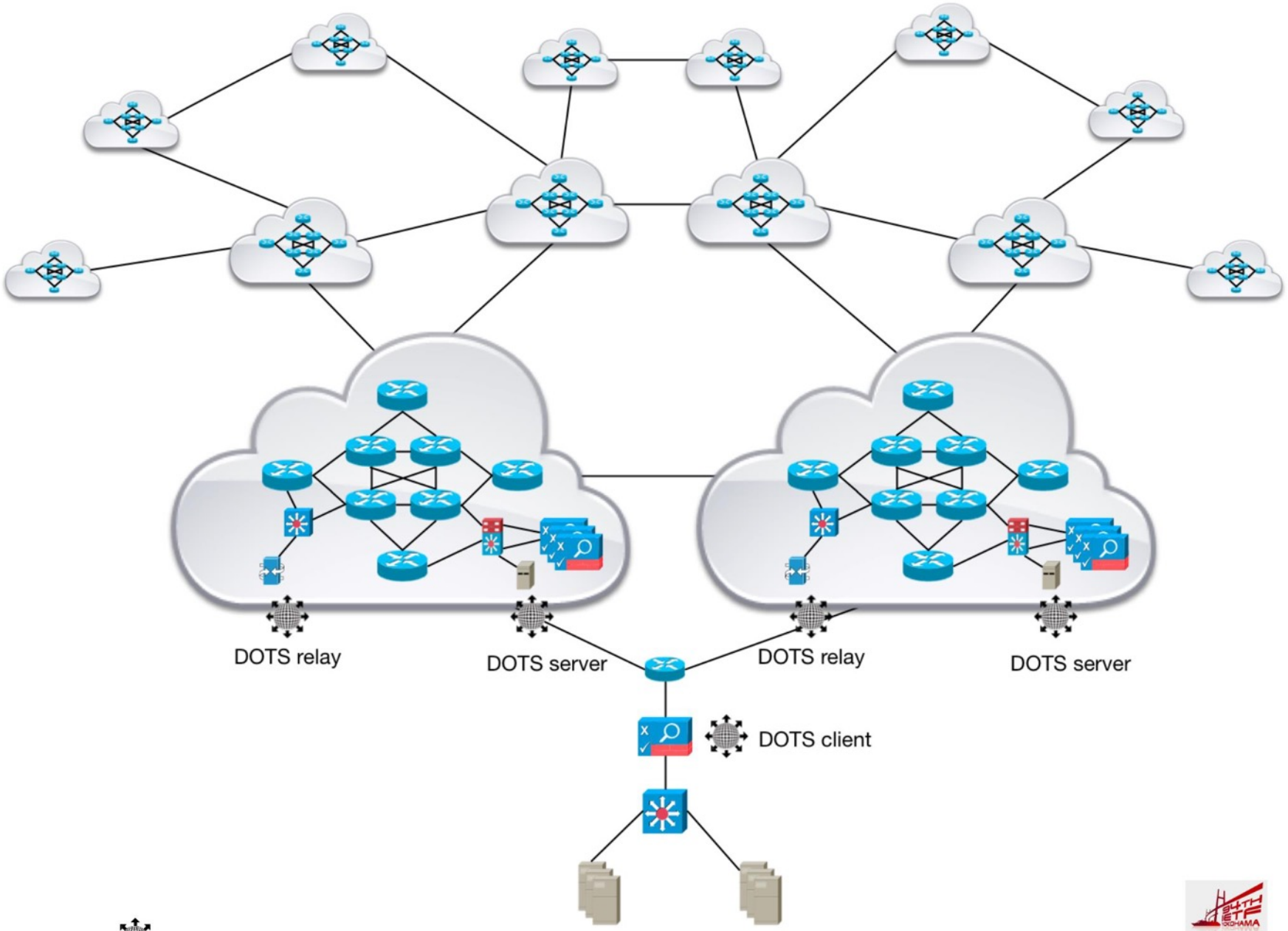
Mitigación en curso.

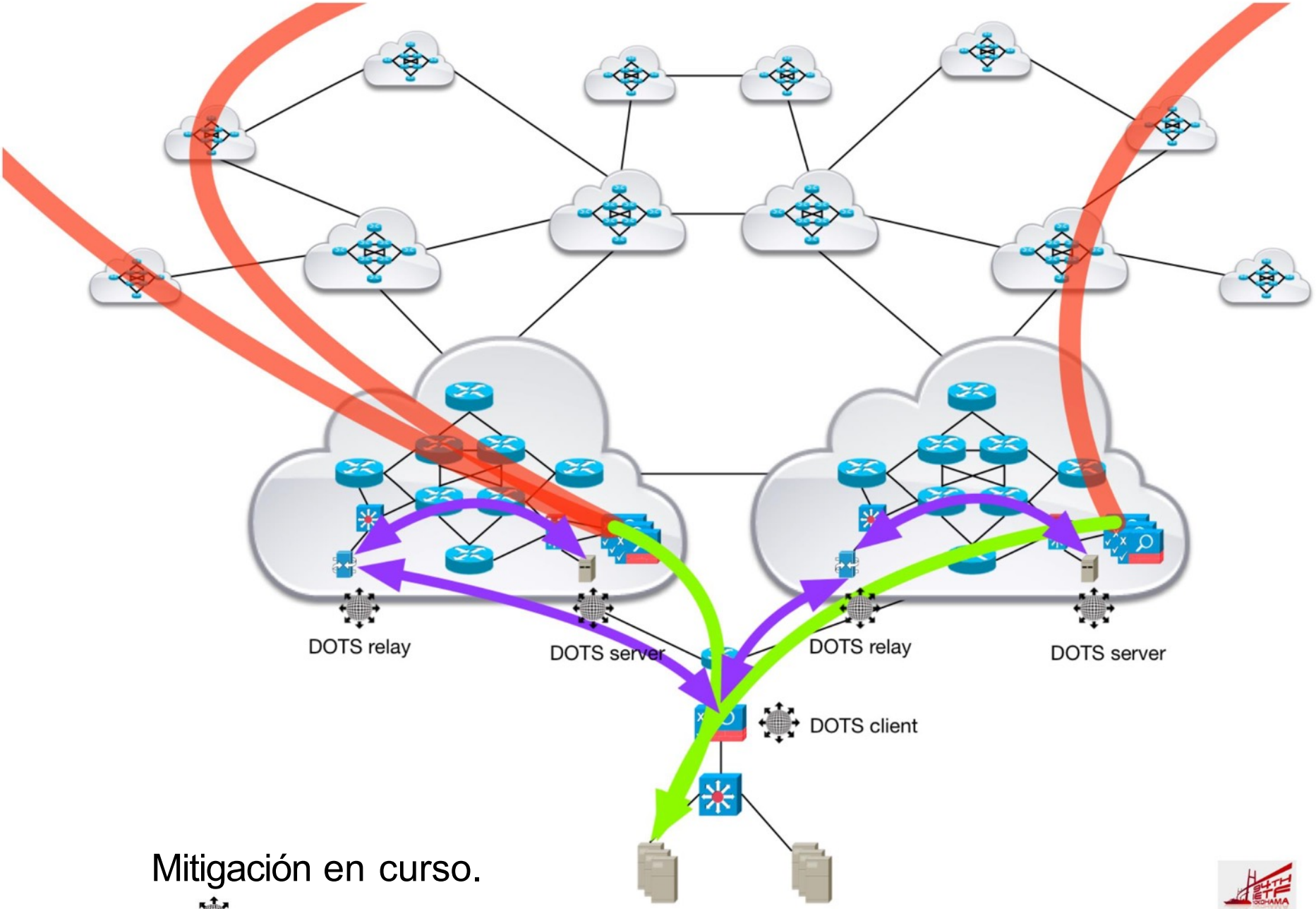


Comunicación DOTS

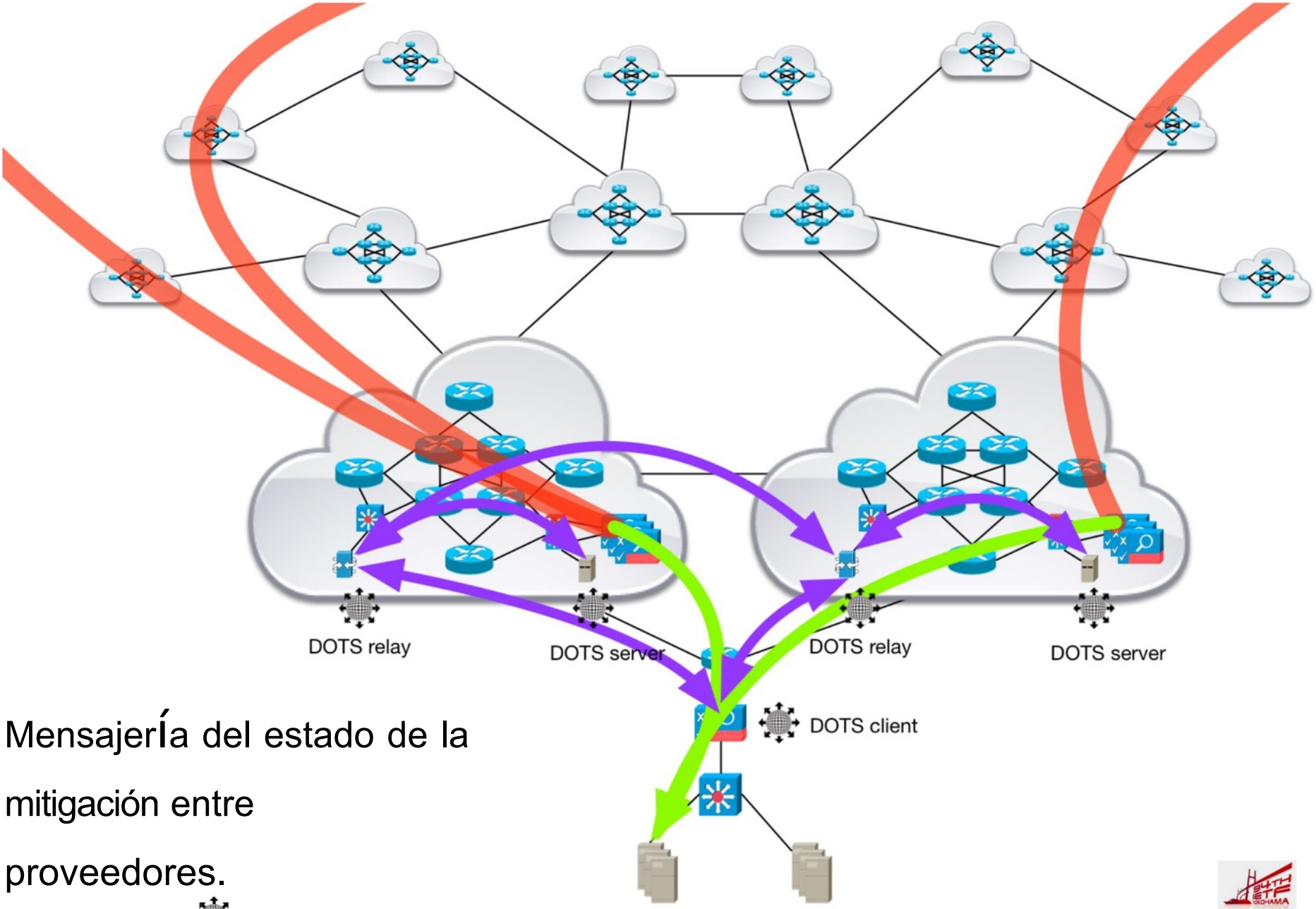
relaciones.

4.1.1 - Variación con Múltiple Proveedores de mitigación de DDoS en sentido ascendente

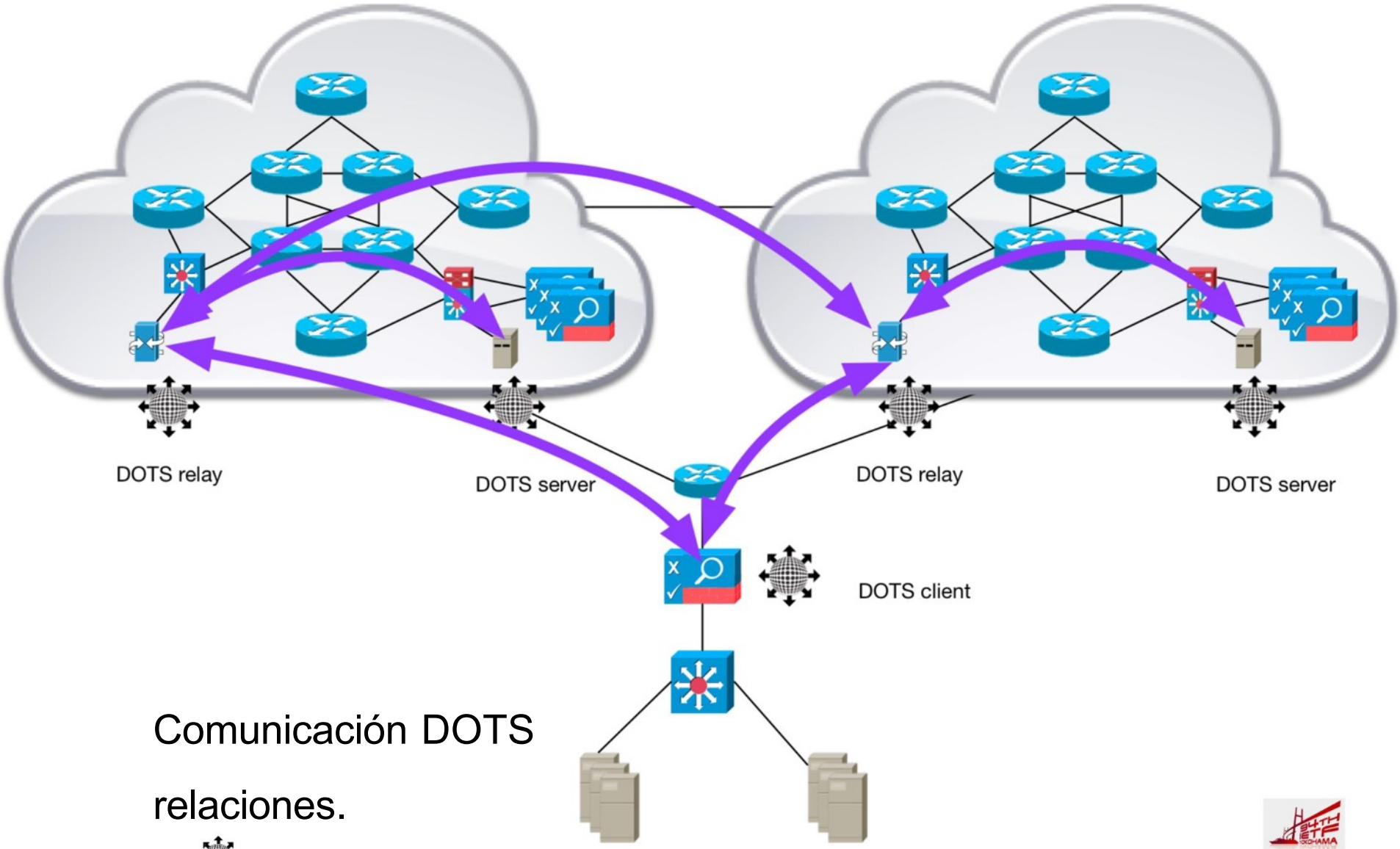

DOTS relay
DOTS server
DOTS relay
DOTS server
DOTS client



Mitigación en curso.



Mensajería del estado de la mitigación entre proveedores.

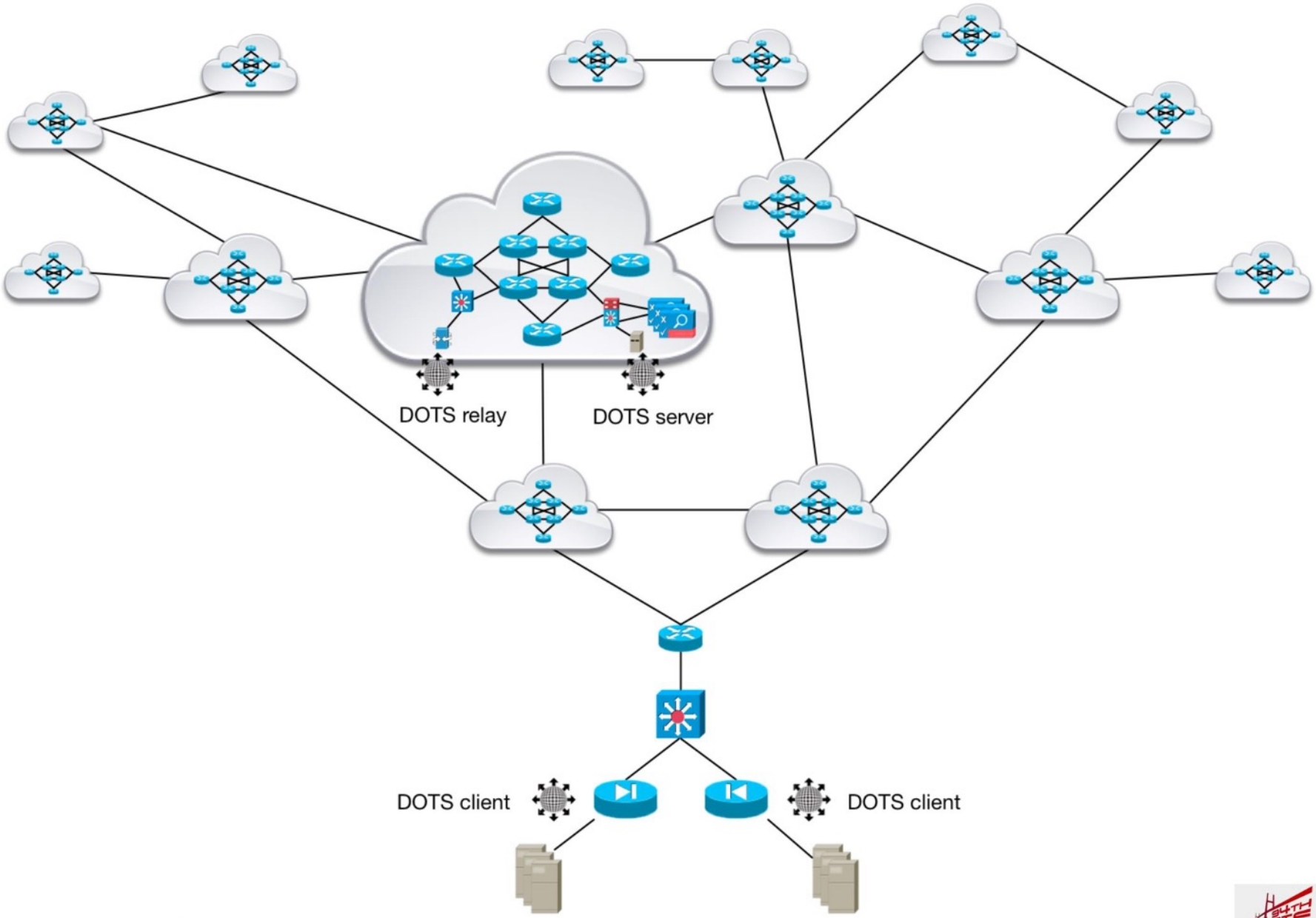


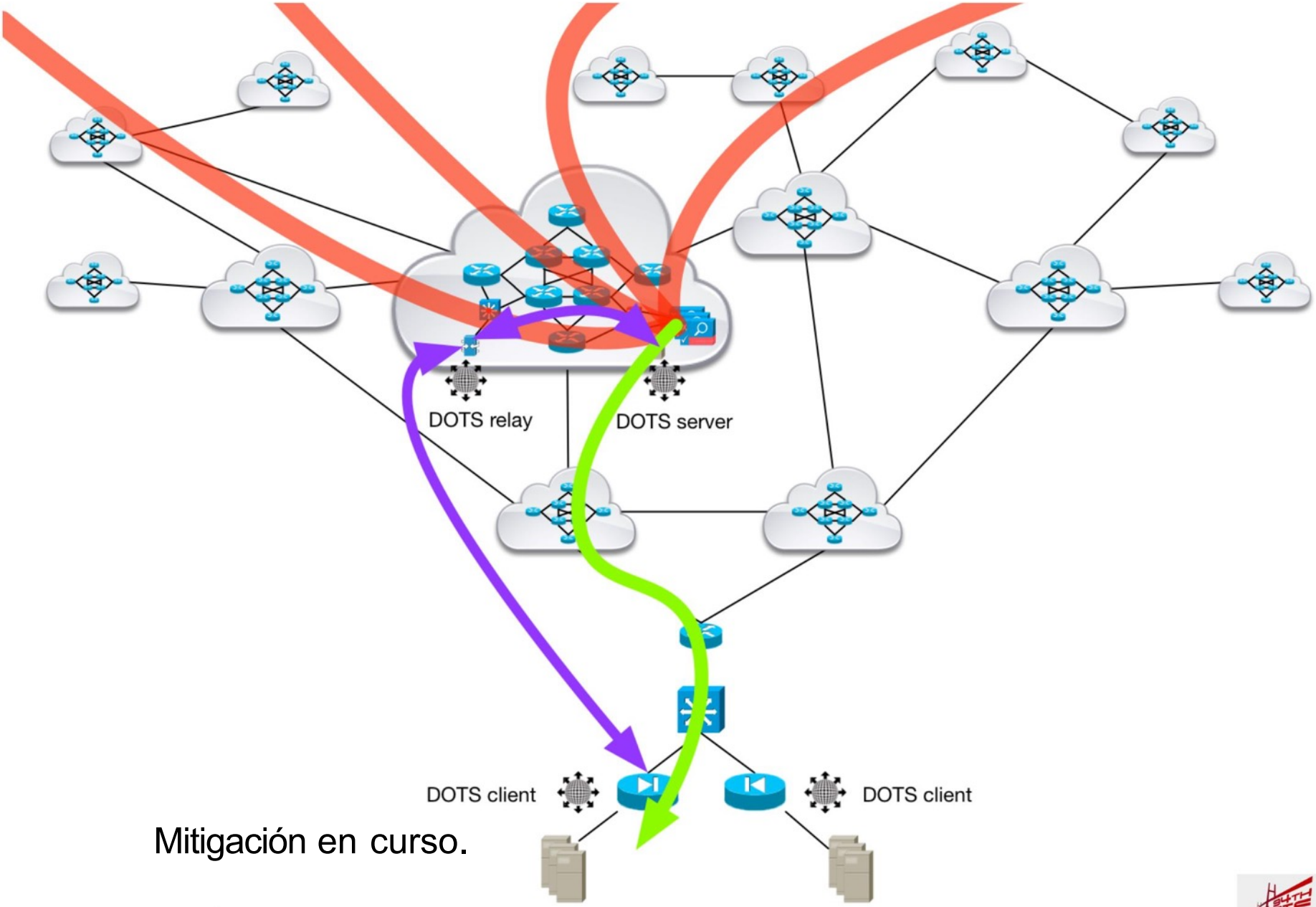
Comunicación DOTS

relaciones.

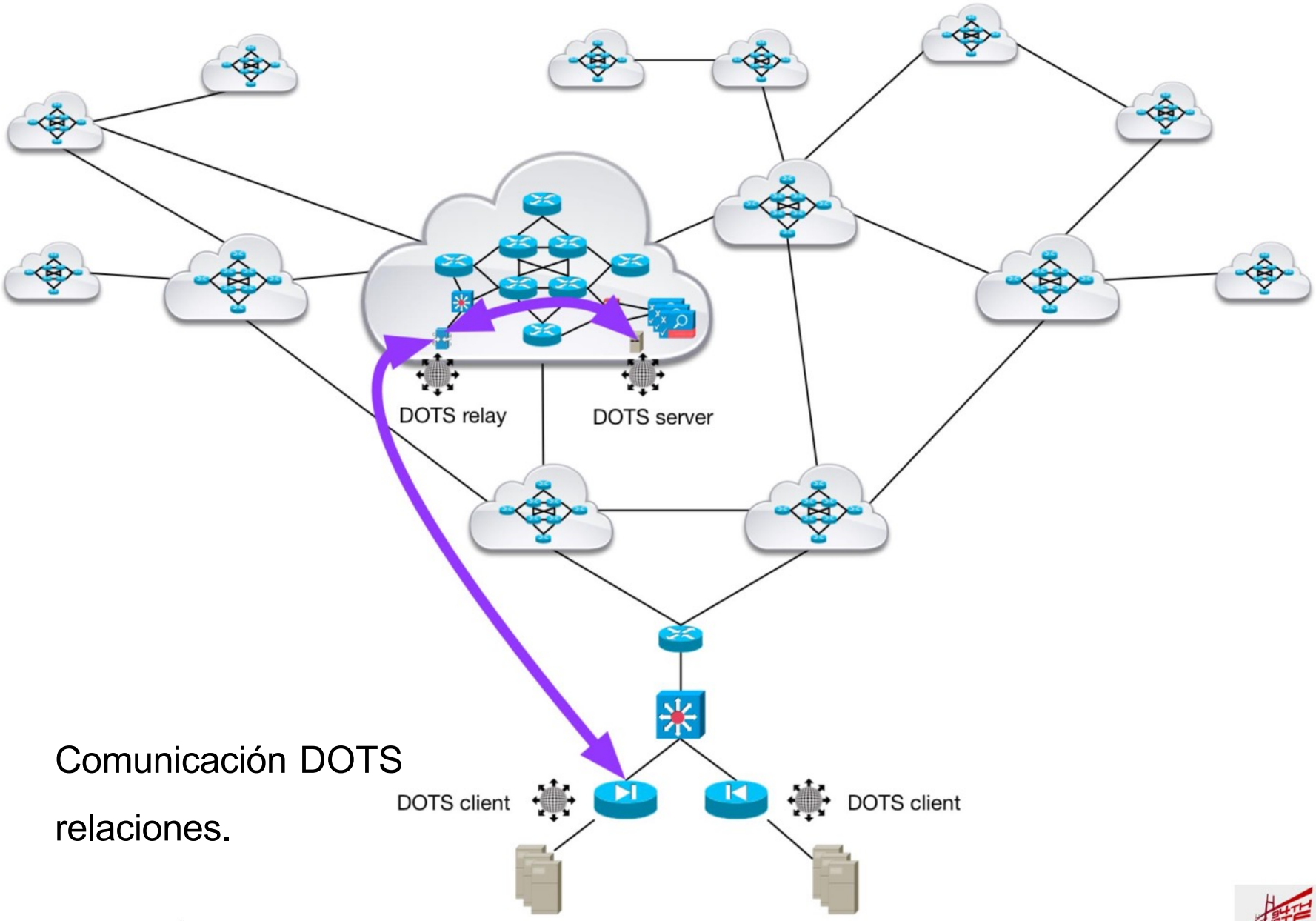
4.1.2 - Infraestructura de red

Dispositivo Solicita DDoS Upstream


DOTS relay
DOTS server
DOTS client
DOTS client



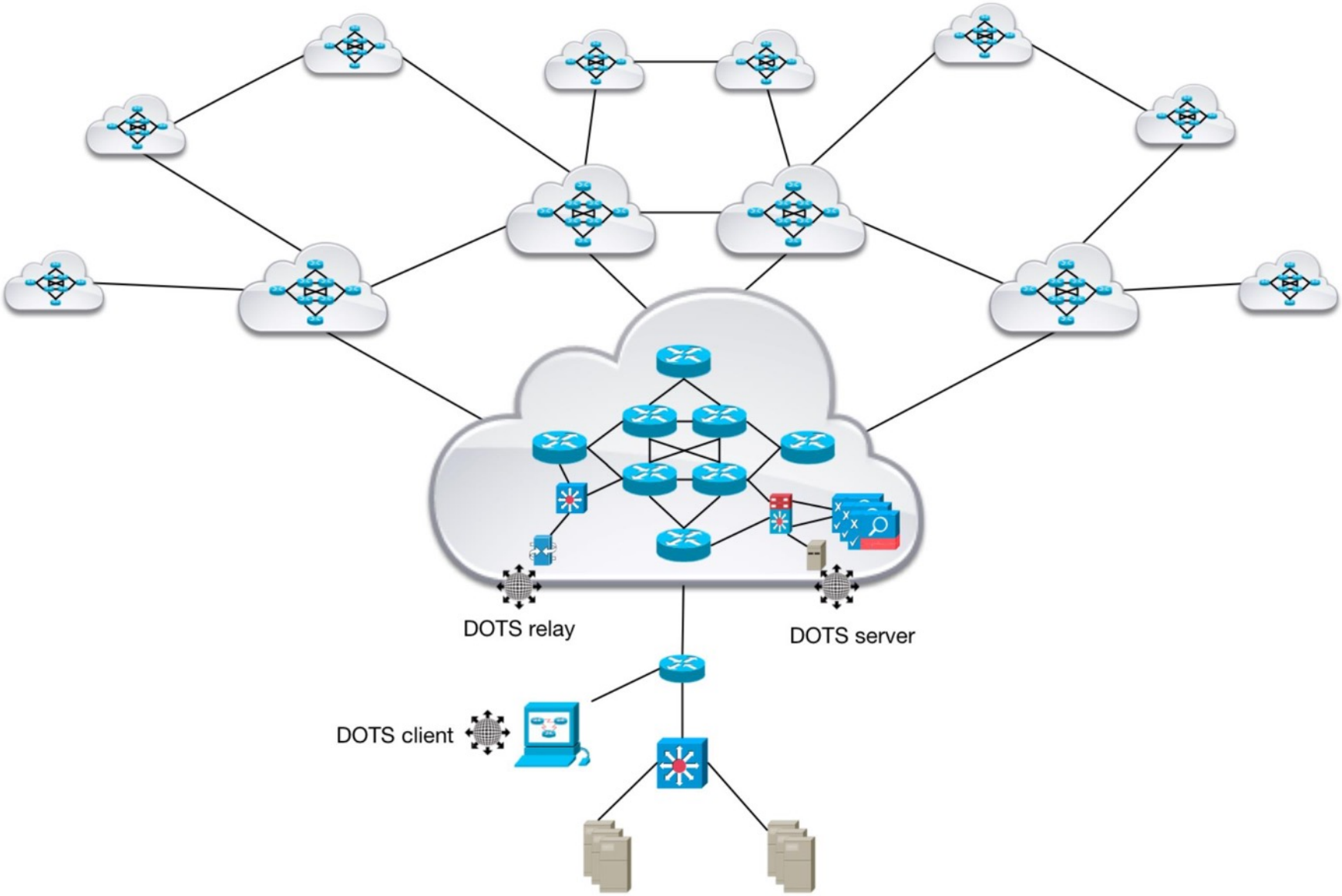
Mitigación en curso.

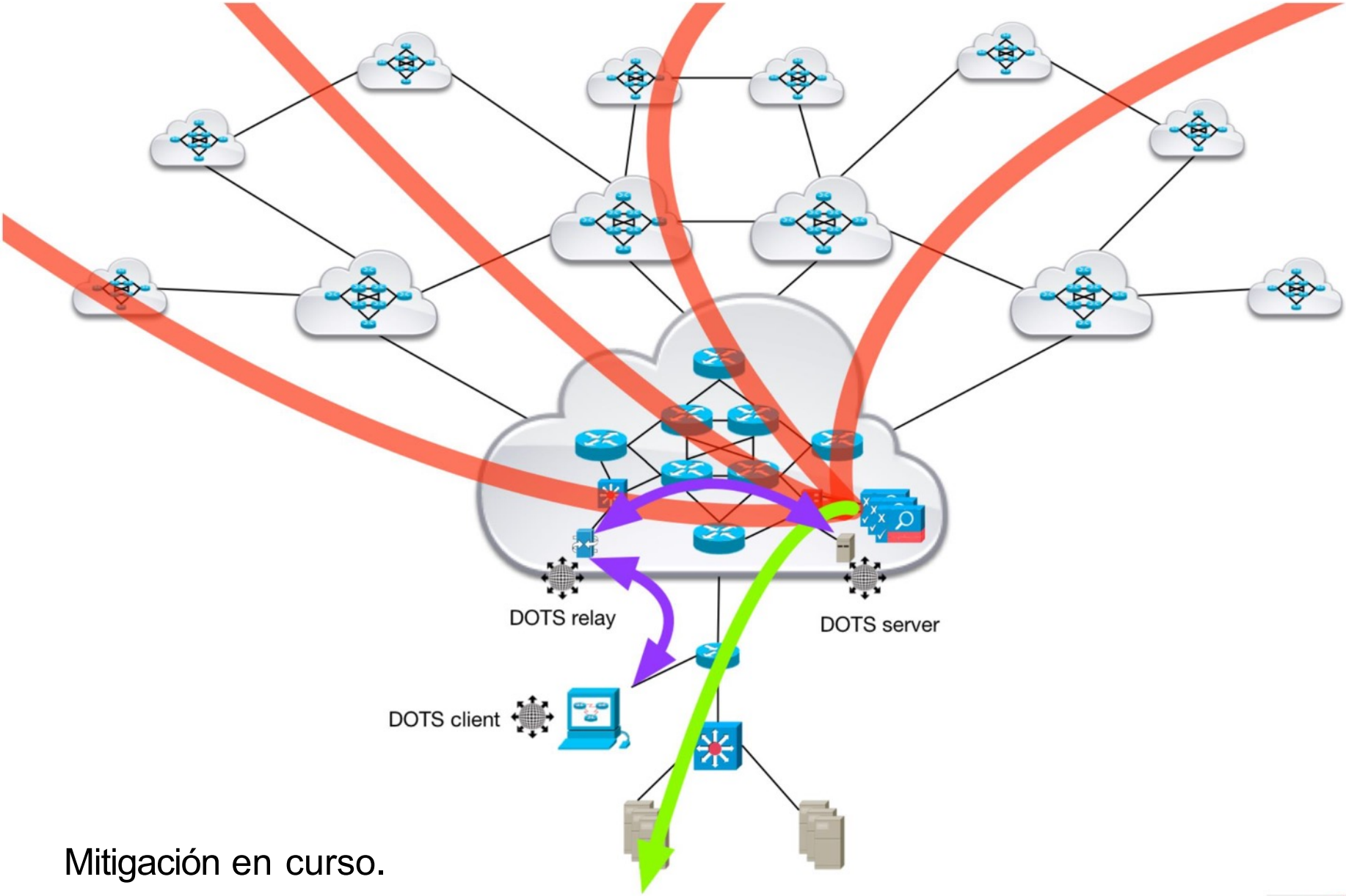


Comunicación DOTS

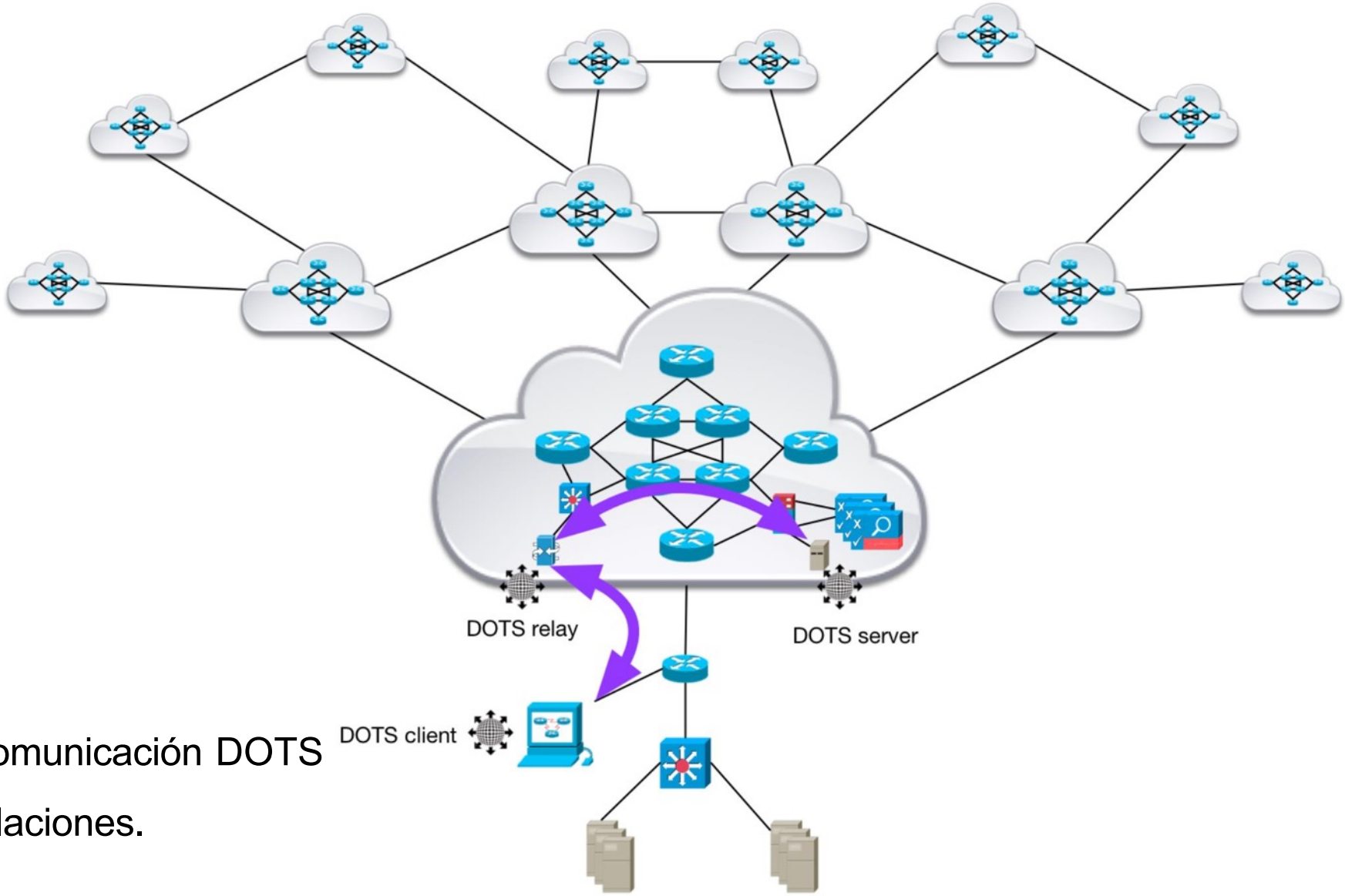
relaciones.

4.1.3 - Detección de telemetría A ack/ Solicitudes de sistemas de clasificación en sentido


DOTS relay
DOTS server
DOTS client



Mitigación en curso.

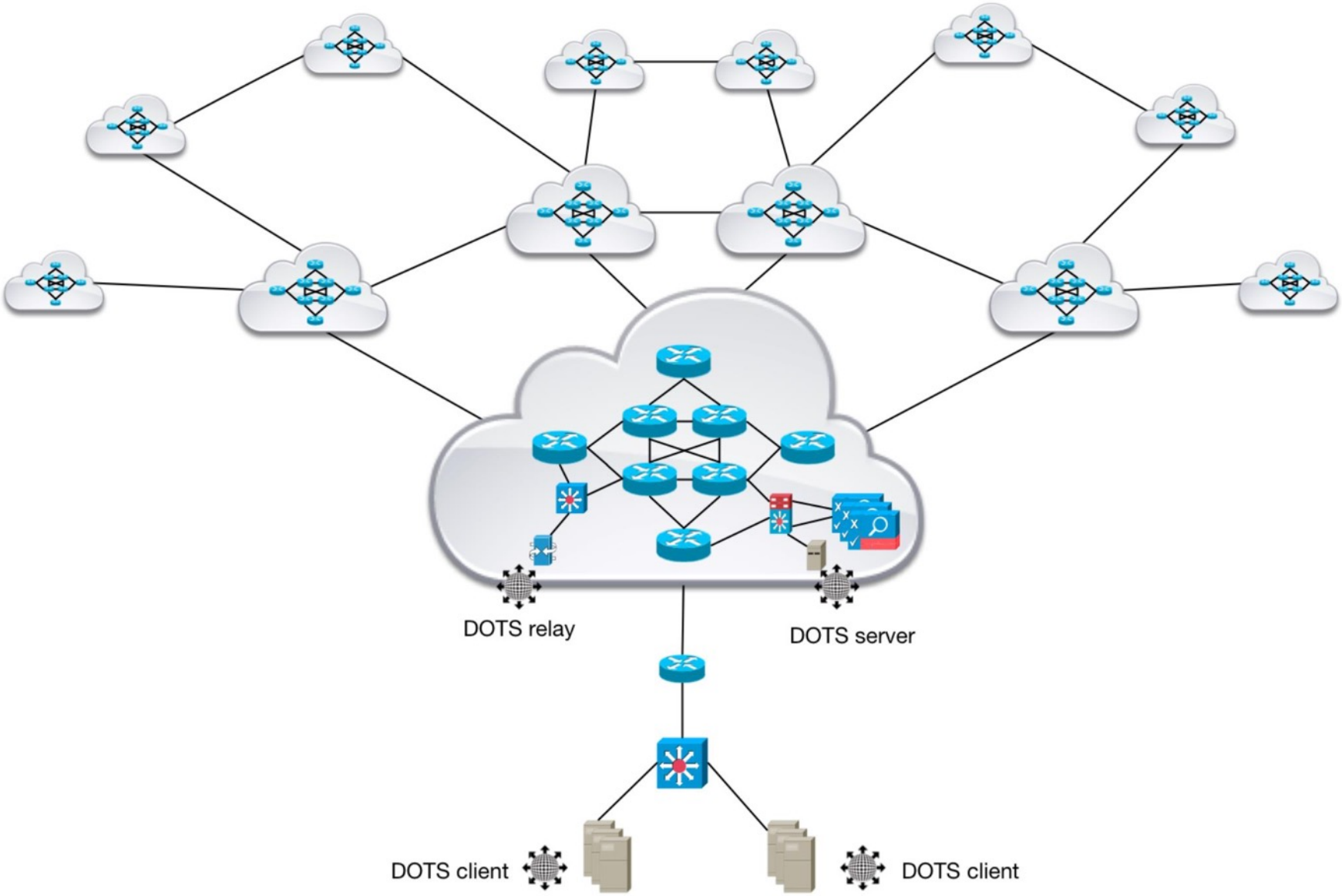


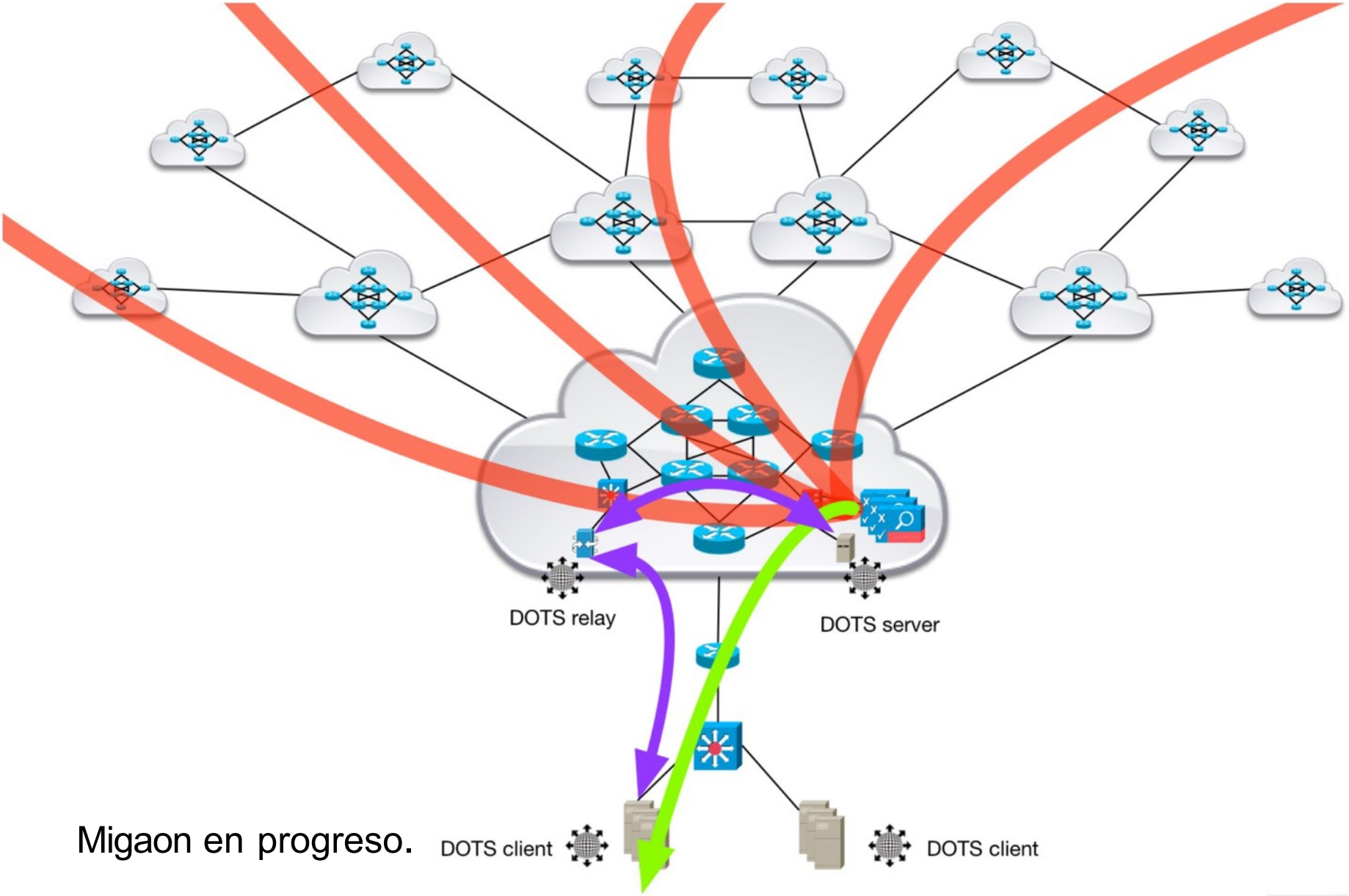
Comunicación DOTS

relaciones.

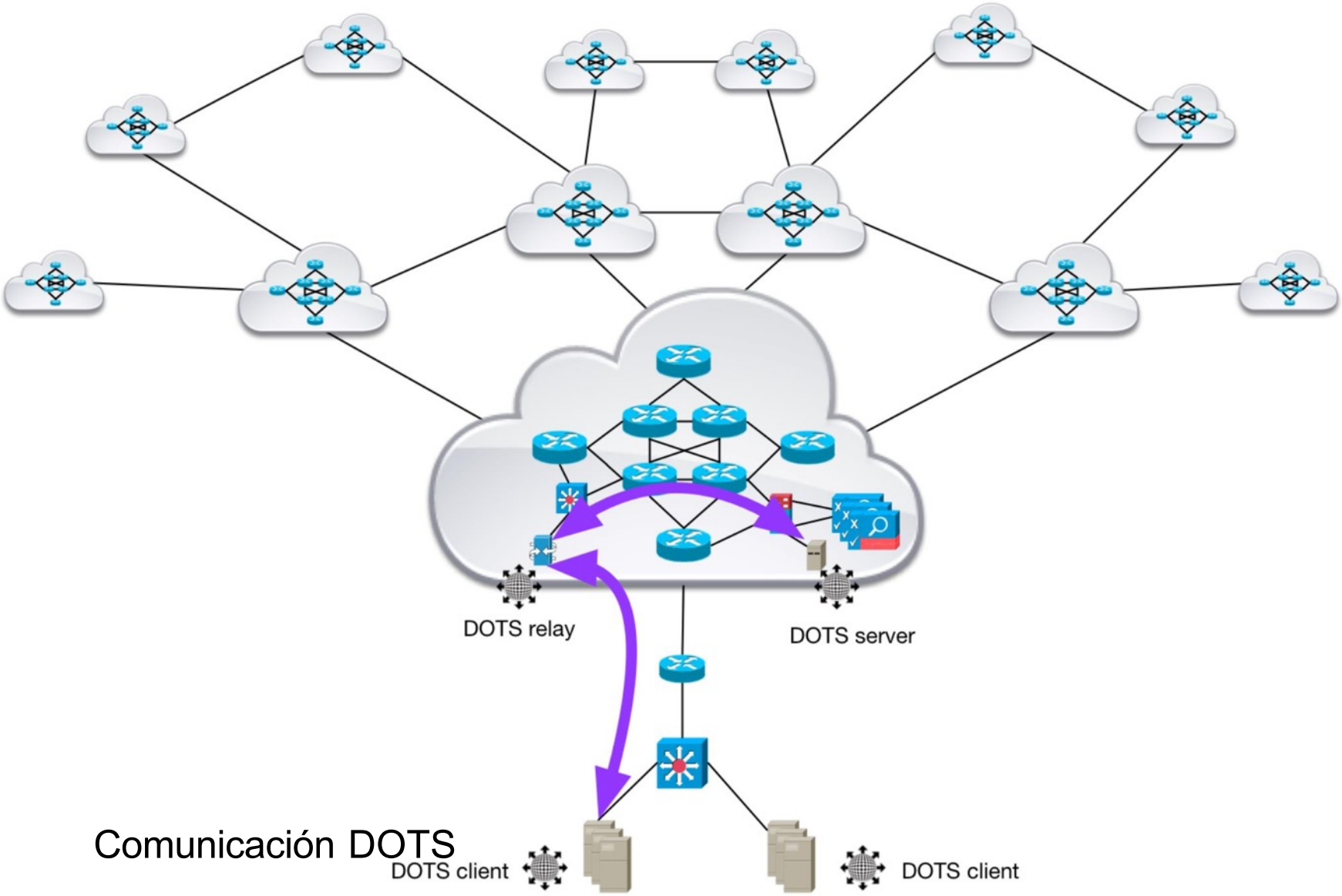
4.1.4 - Servicio/Aplicación dirigido

Solicitudes de mitigación de DDoS en sentido ascendente


DOTS relay
DOTS server
DOTS client
DOTS client



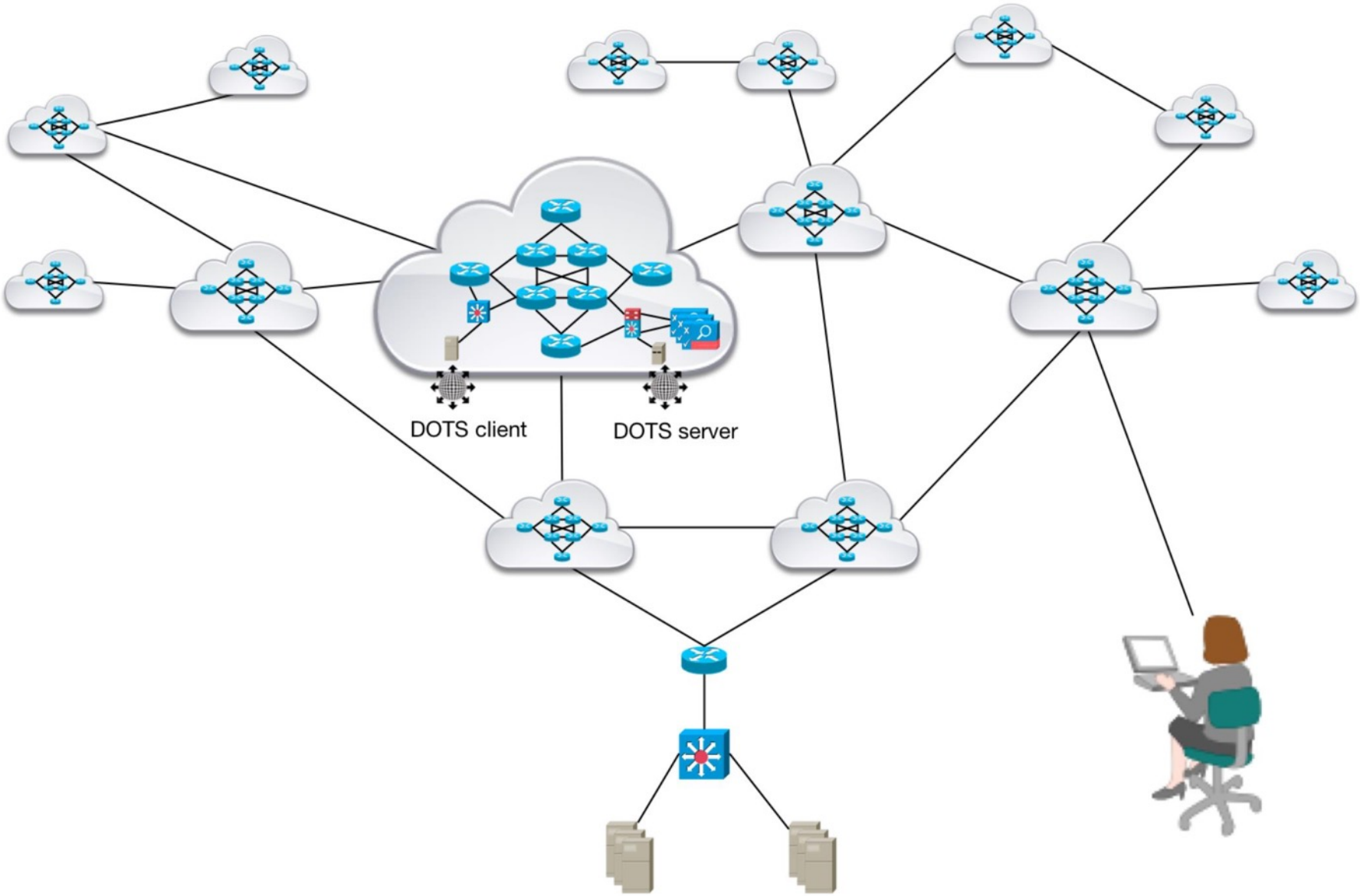
Migaon en progreso.

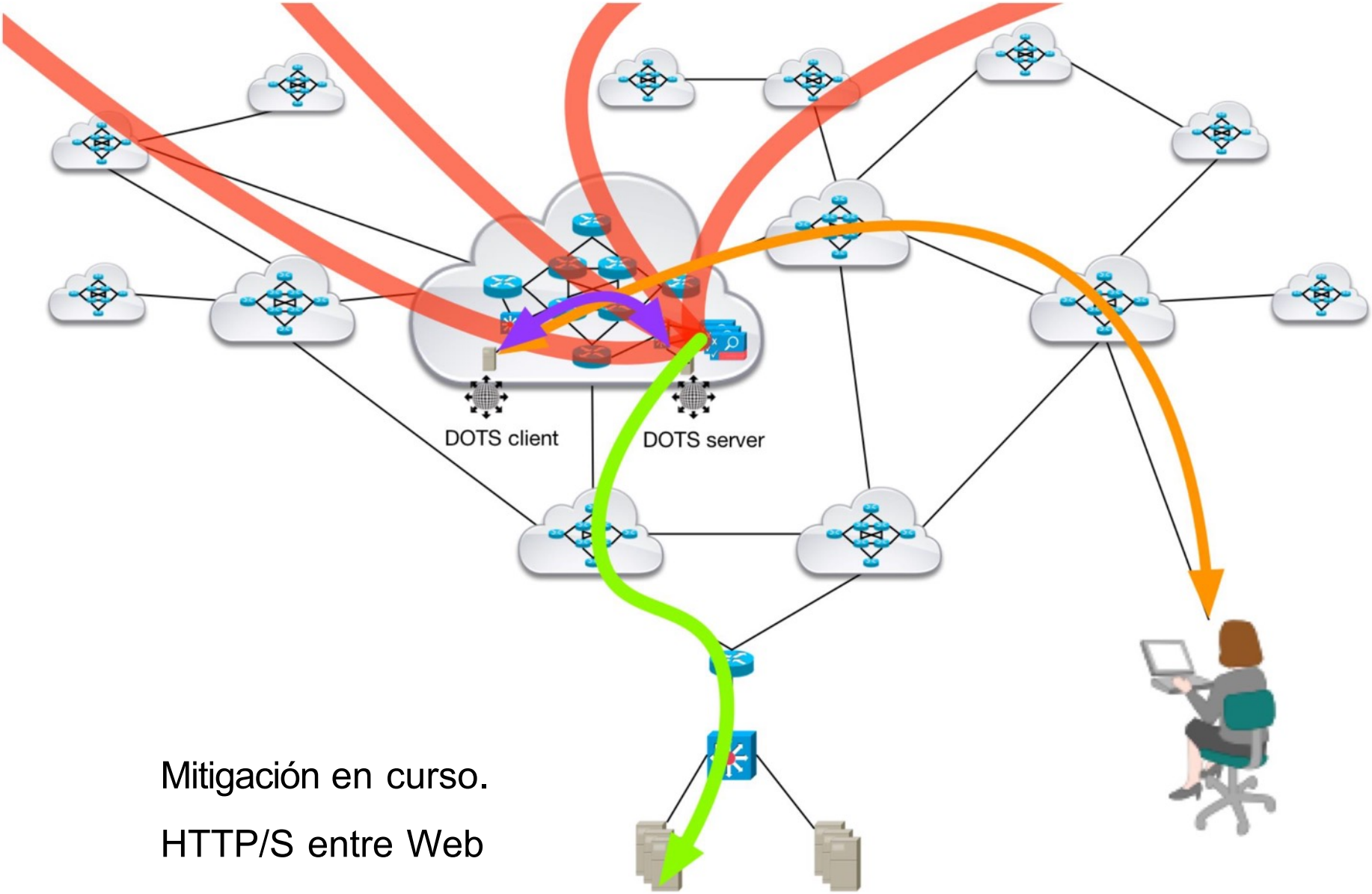


Comunicación DOTS

relaciones.

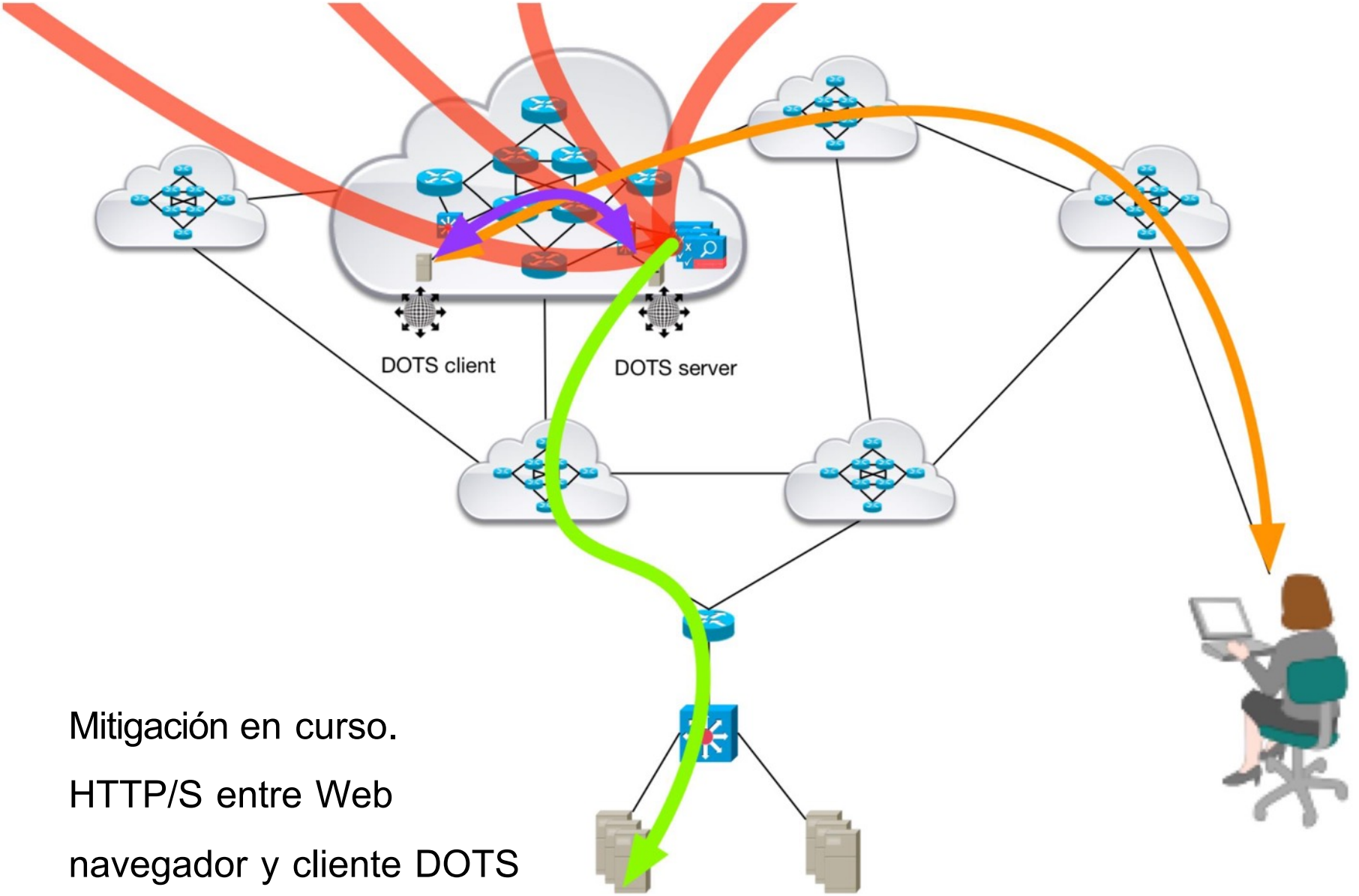
4.1.5 - Solicitud manual del portal web a Mitigador de aguas arriba


DOTS client
DOTS server



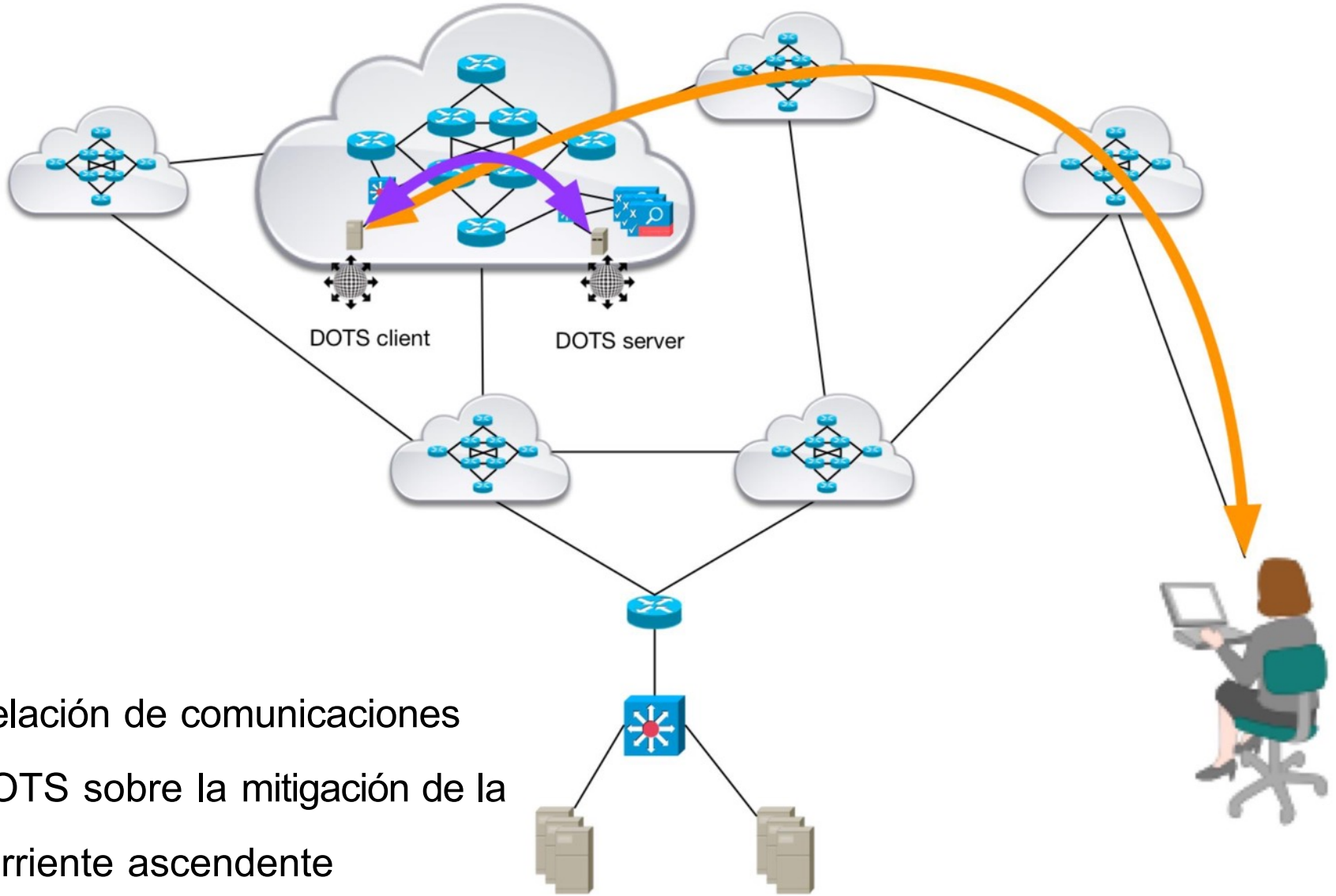
Mitigación en curso.

HTTP/S entre Web navegador y cliente DOTS en el portal web.



Mitigación en curso.

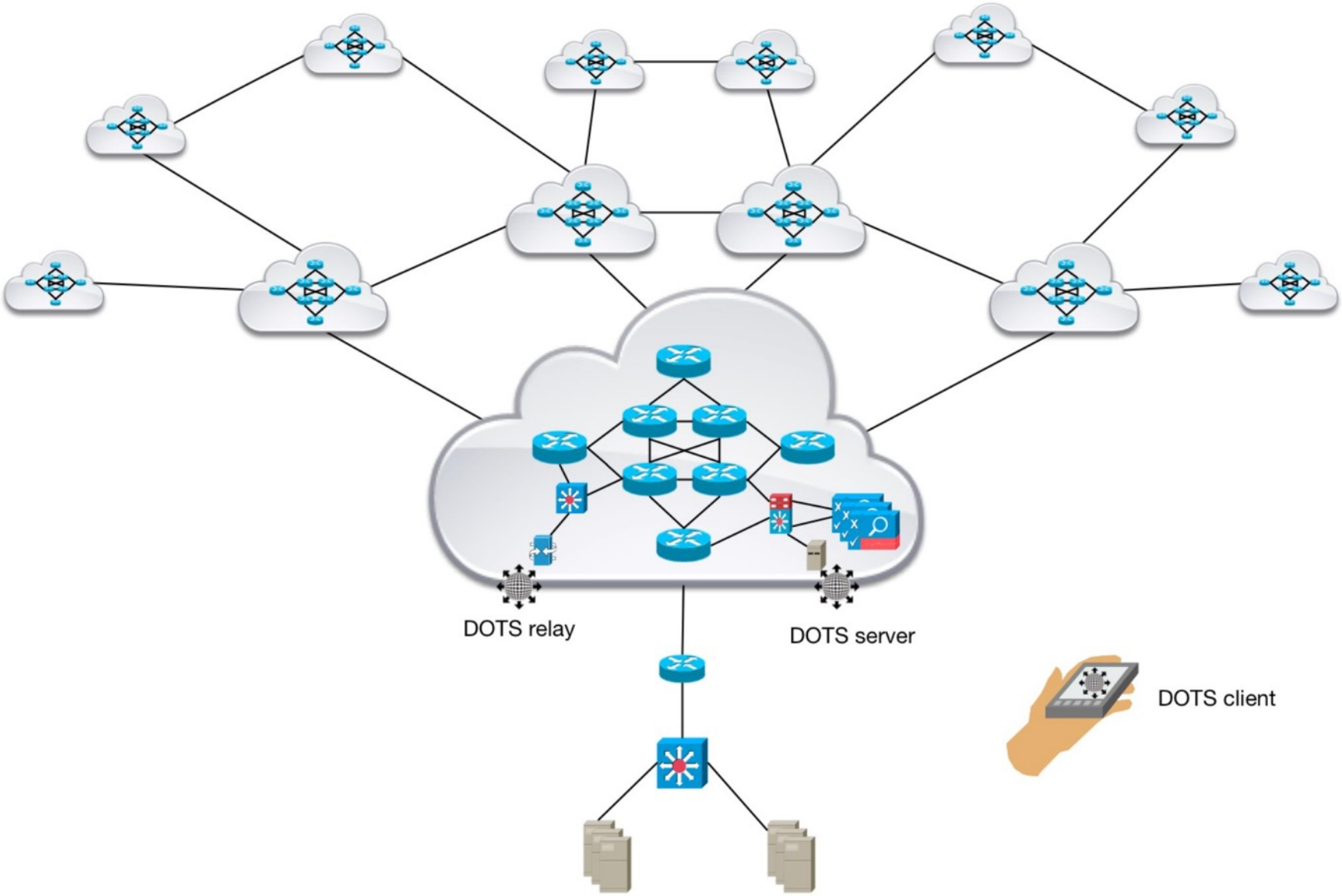
HTTP/S entre Web navegador y cliente DOTS en el portal web.

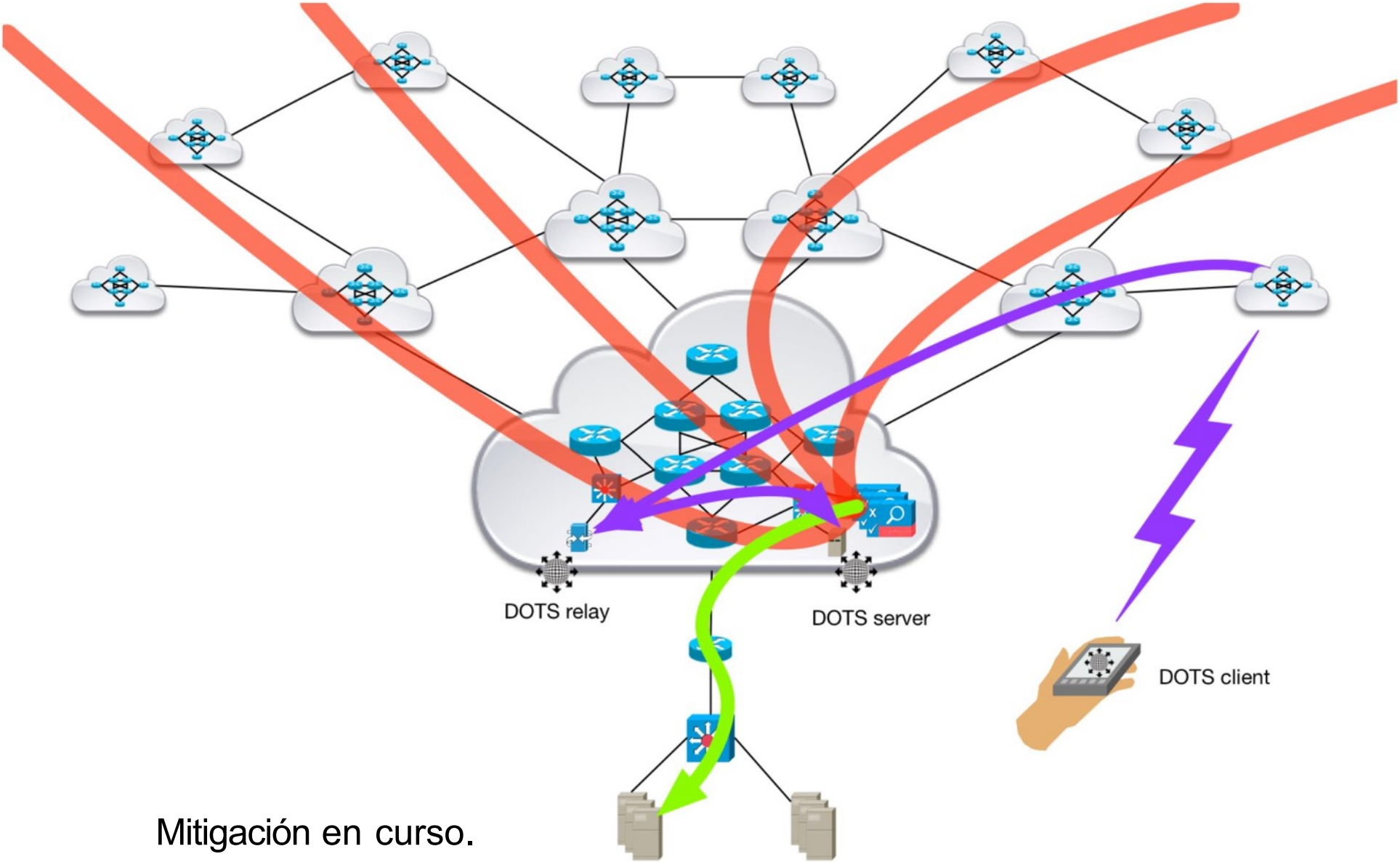


Relación de comunicaciones DOTS sobre la mitigación de la corriente ascendente sólo en la red.

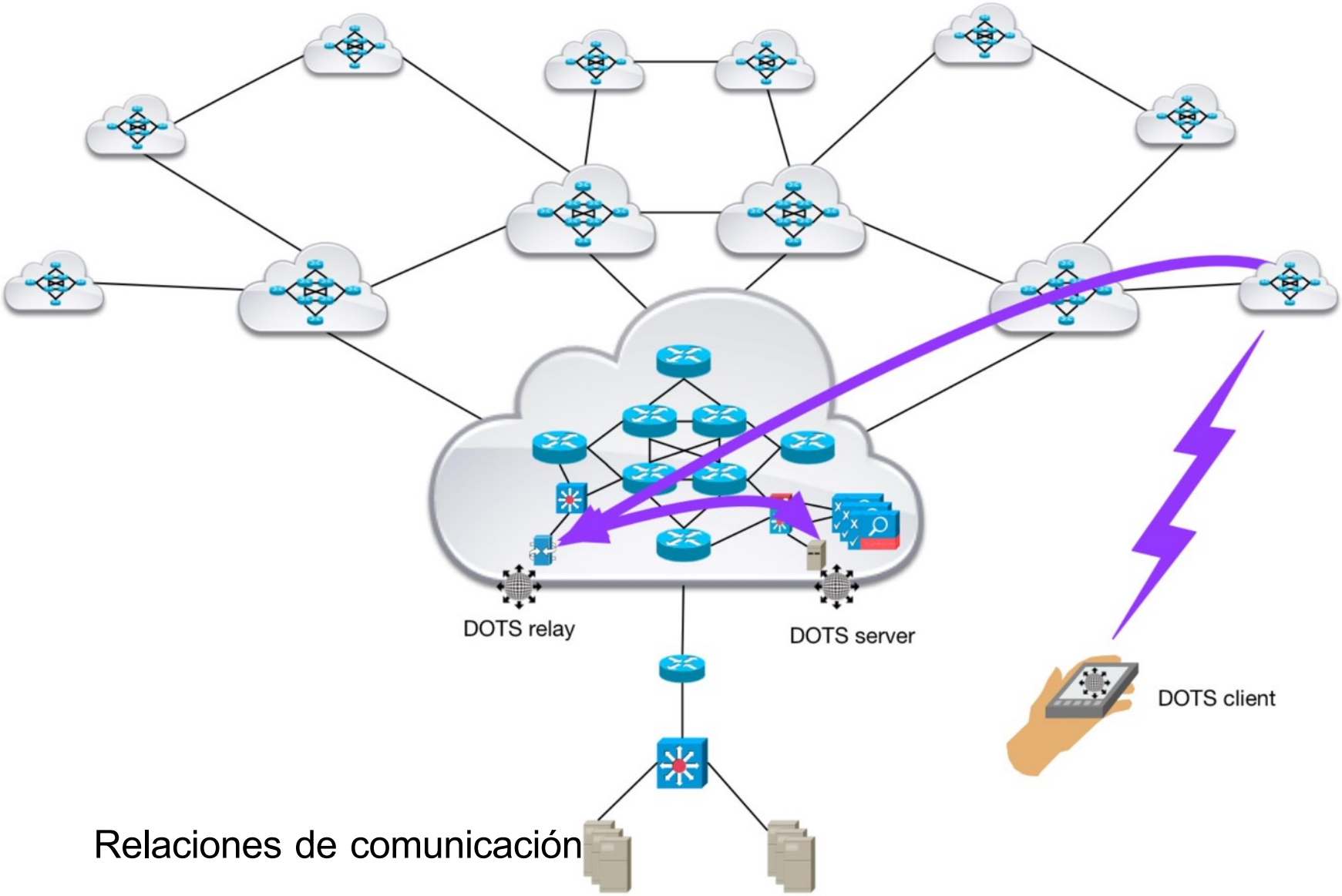
4.1.6 - Dispositivo móvil manual

Solicitud de aplicación a la corriente


DOTS relay
DOTS server
DOTS client



Mitigación en curso.

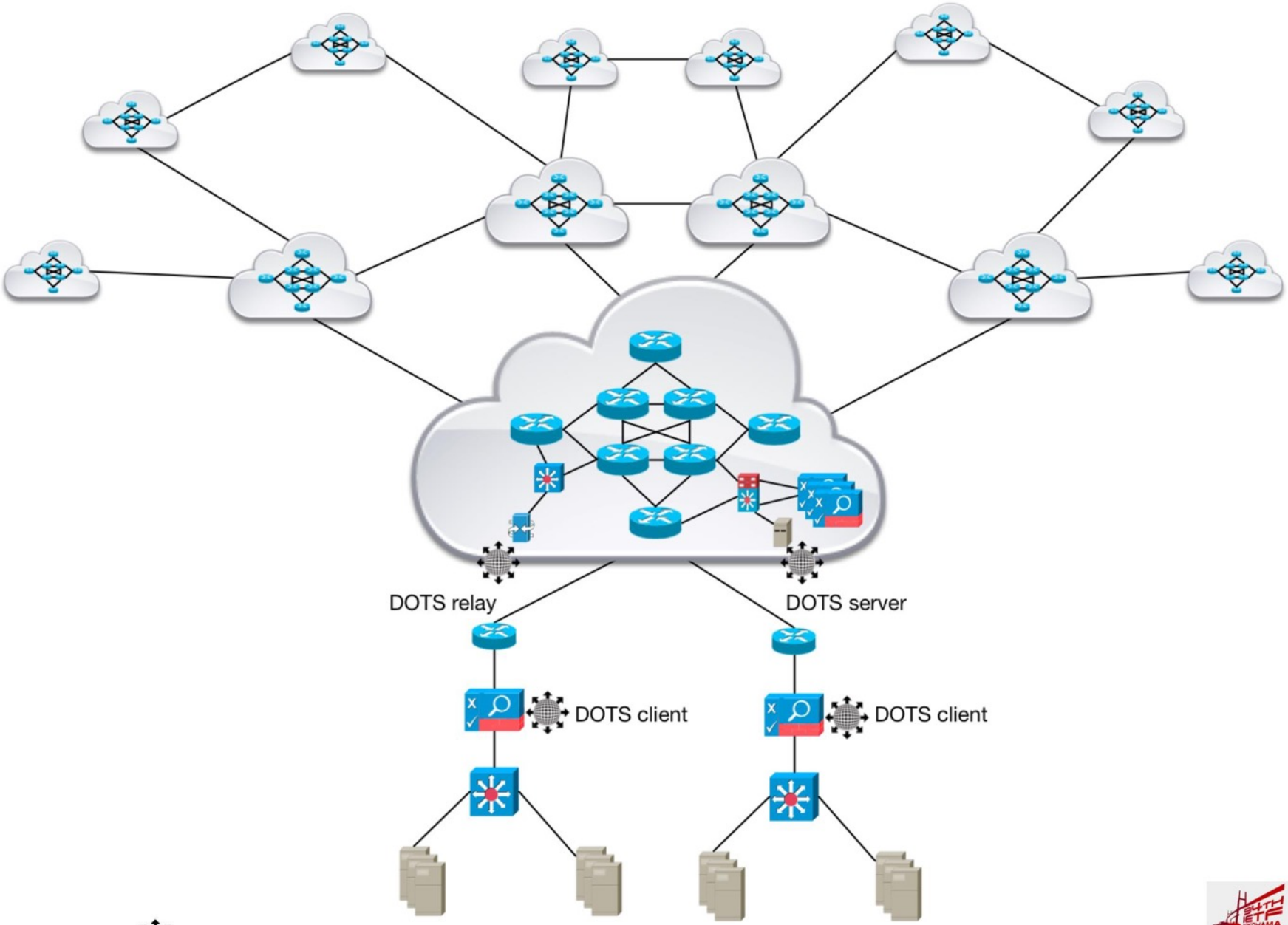


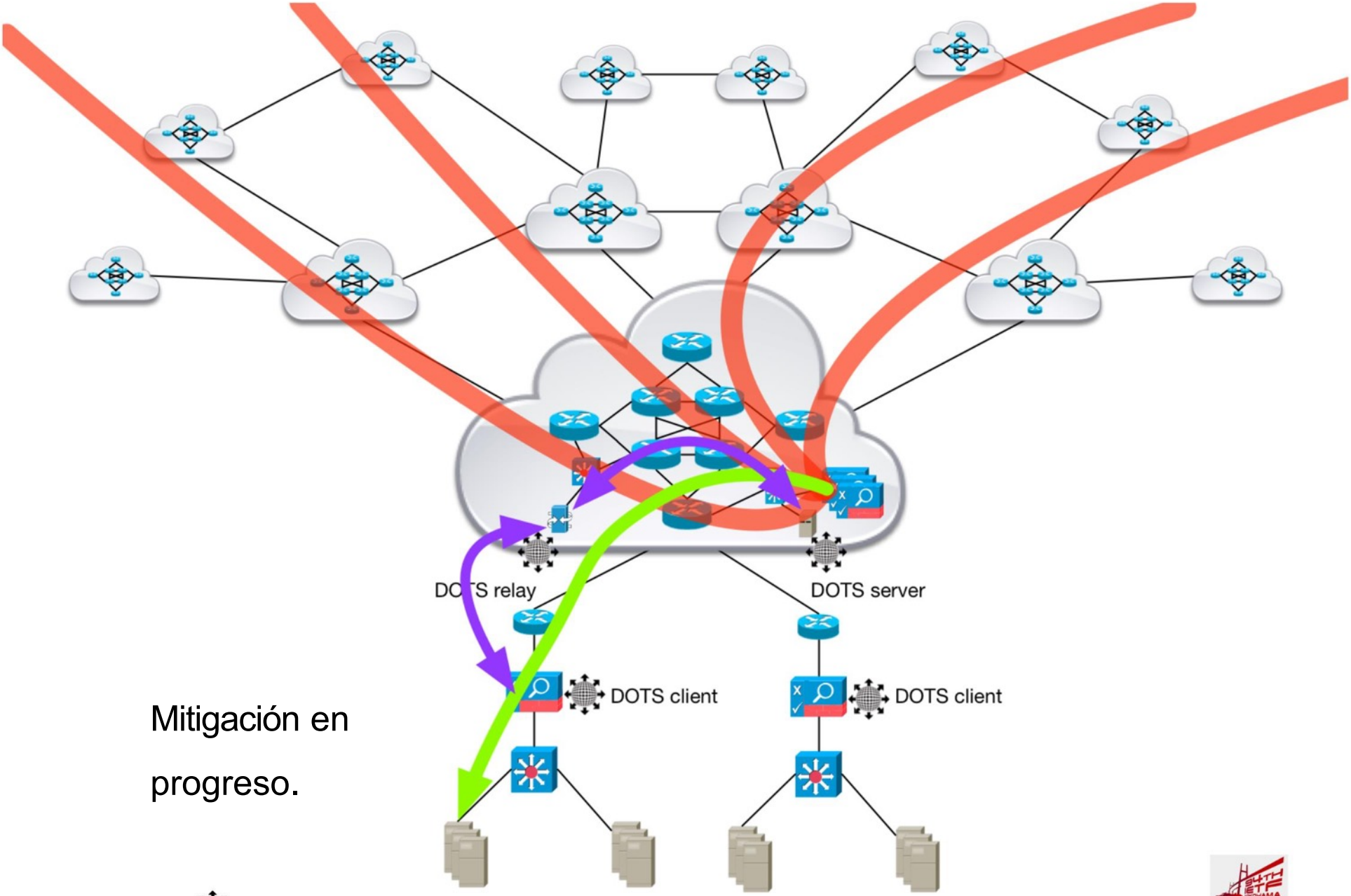
Relaciones de comunicación

DOTS

4.1.7 - CPE o PE sin éxito

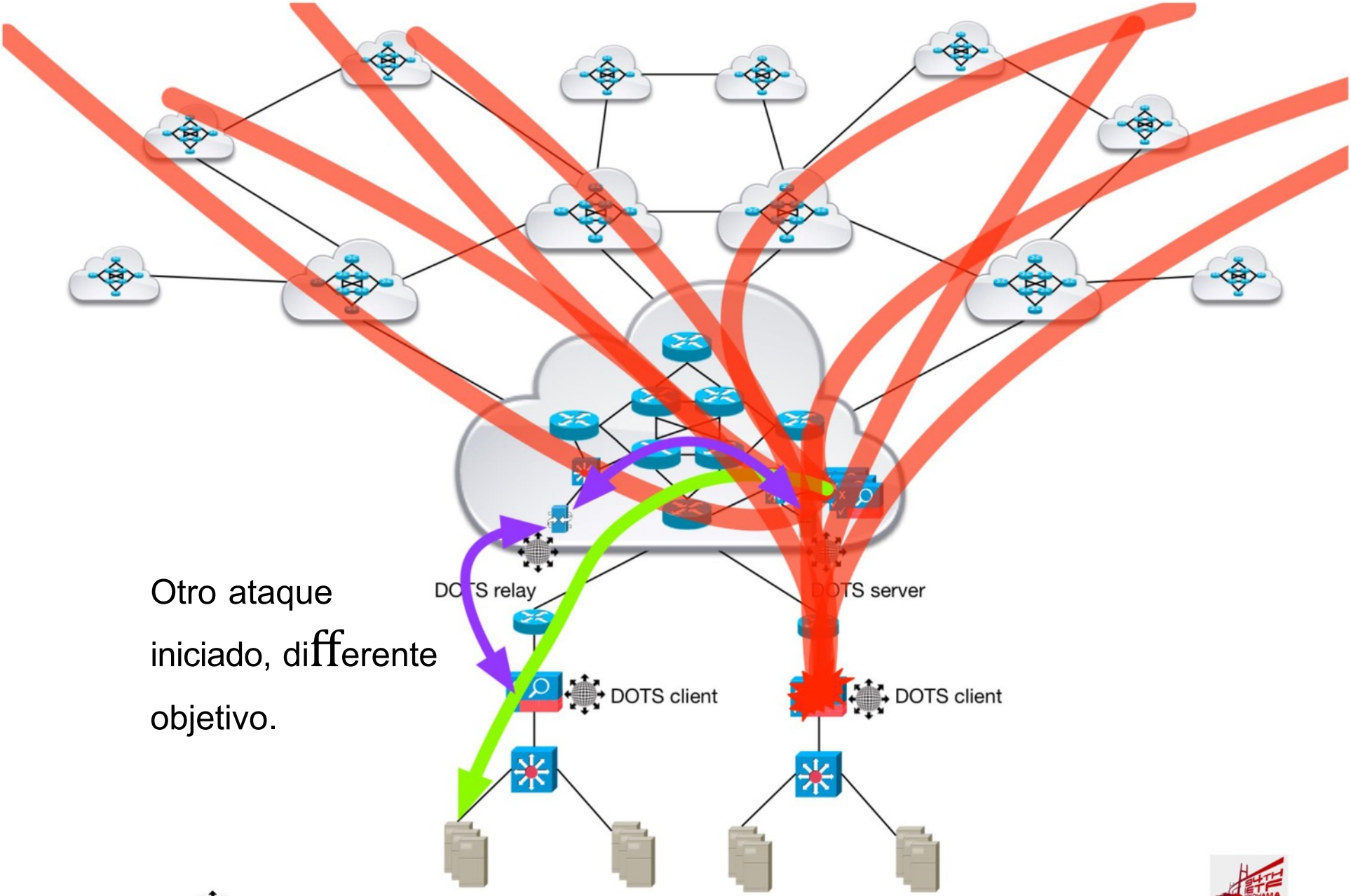
Petición de mitigación para la corriente

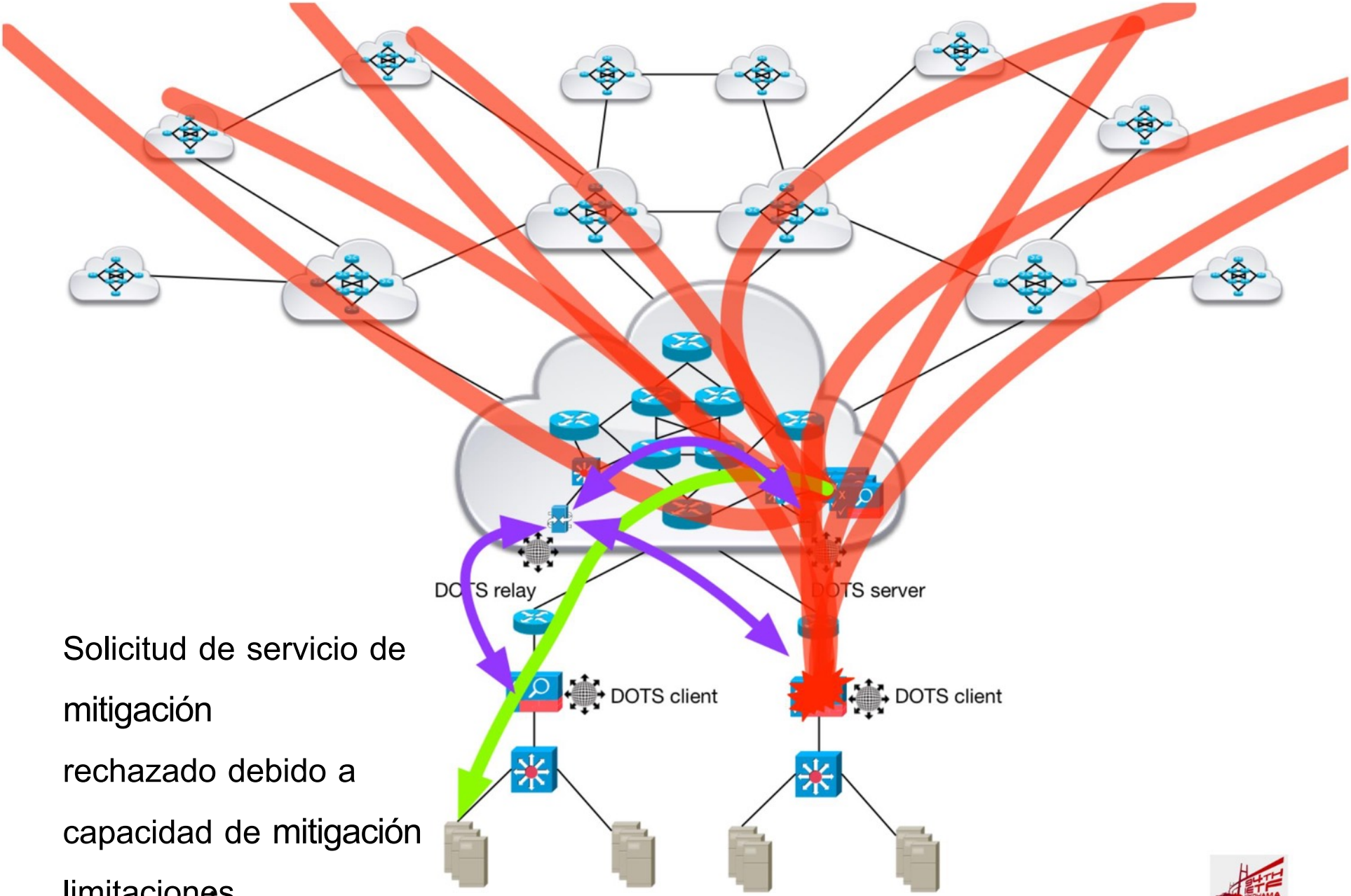

DOTS relay
DOTS server
DOTS client
DOTS client



Mitigación en progreso.

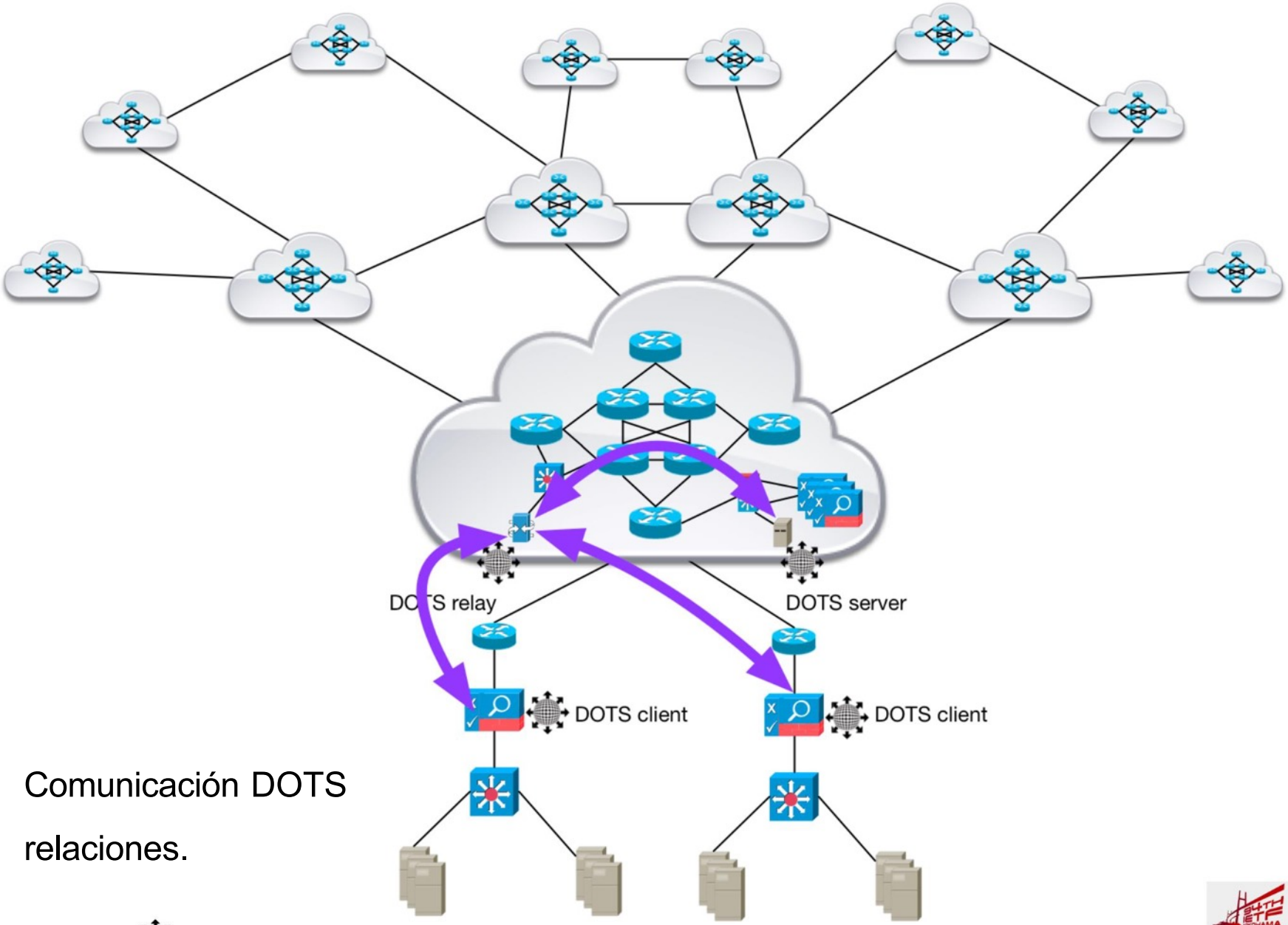
Otro ataque iniciado, different objetivo.





Solicitud de servicio de mitigación

rechazado debido a capacidad de mitigación limitaciones.



Comunicación DOTS

relaciones.

4.2 - Casos de uso auxiliares

4.2.1 - Registro automático

- Más allá de las solicitudes de mitigación de ataques, las respuestas y el estado mensajes, los DOTS también pueden ser útiles para la administración tareas.
- Las tareas administrativas son un importante obstáculo para la eficacia de la Mitigación de DDoS.
- Los clientes de DOTS con las credenciales adecuadas pueden registrarse automáticamente con los servidores DOTS en las redes de mitigación ascendentes.
- Esto ayuda a la incorporación del servicio de mitigación de DDoS, movimientos/agregados/cambios.

4.2.2 - Aprovisionamiento automático de contramedidas DDoS

- El aprovisionamiento de contramedidas DDoS hoy en día es un proceso en gran medida proceso manual, los errores y la ineficacia pueden ser problemáticos.

- Esto puede llevar a una mitigación de DDoS inadecuada
  servicios que a menudo no están optimizados para los activos en
  Protección DDoS. La rapidez de la mitigación, la eficacia se resiente.

- La incorporación de las organizaciones durante un ataque - una
  situación común- puede ser muy desafiante.

- El carácter "autodescriptivo" del registro DOTS y
  Las solicitudes de estado de mitigación pueden aprovecharse para automatizar el proceso de selección, aprovisionamiento y ajuste de contramedidas.

- Comentarios sobre la eficacia de la mitigación de los clientes de DOTS a DOTS
  servidores durante un ataque puede ser aprovechado para
  ajuste y optimización de la mitigación.

4.2.3 - Notificación informativa de ataques DDoS a terceros

- Además de las solicitudes de servicio de las organizaciones bajo ataque a los mitigadores de aguas arriba, DOTS puede utilizarse para enviar Notificación de ataques DDoS y mensajes de estado a los interesados y terceros autorizados.

- En algunas circunstancias, puede ser beneficioso que se aplique automáticamente Proporcionar notificaciones de ataques y mensajes de estado econdicio o terciarios de mitigación "de respaldo", la seguridad investigadores, proveedores, organismos de seguridad, organismos reguladores agencias, etc.

- Cualquier intercambio de información con terceros debe Sólo se puede llevar a cabo de acuerdo con todas las leyes pertinentes, normativa, obligaciones contractuales, privacidad y acuerdos de confidencialidad.

Próximos pasos para los casos de uso