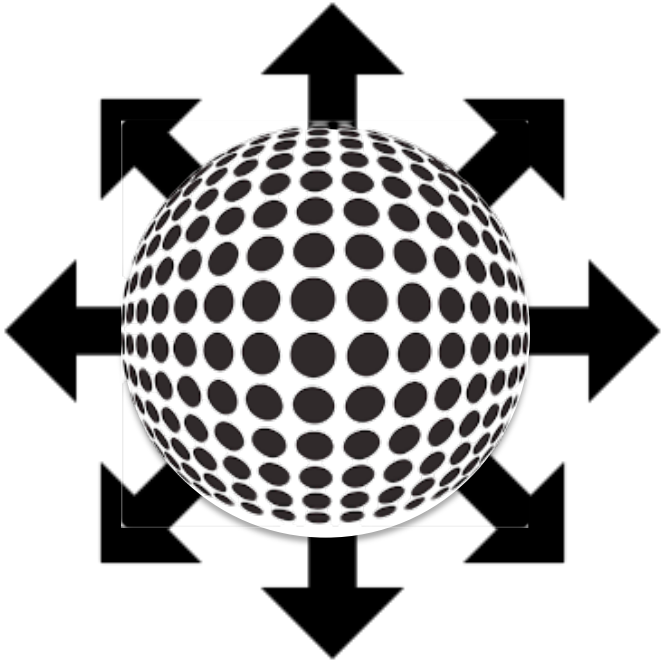


94th IETF
YOKOHAMA JAPAN
1-6 NOVEMBER 2015

分布式拒绝服务开放威胁信令（DOTS）工作组

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

介绍和背景

draft-ietf-dots-use-cases-00 总结

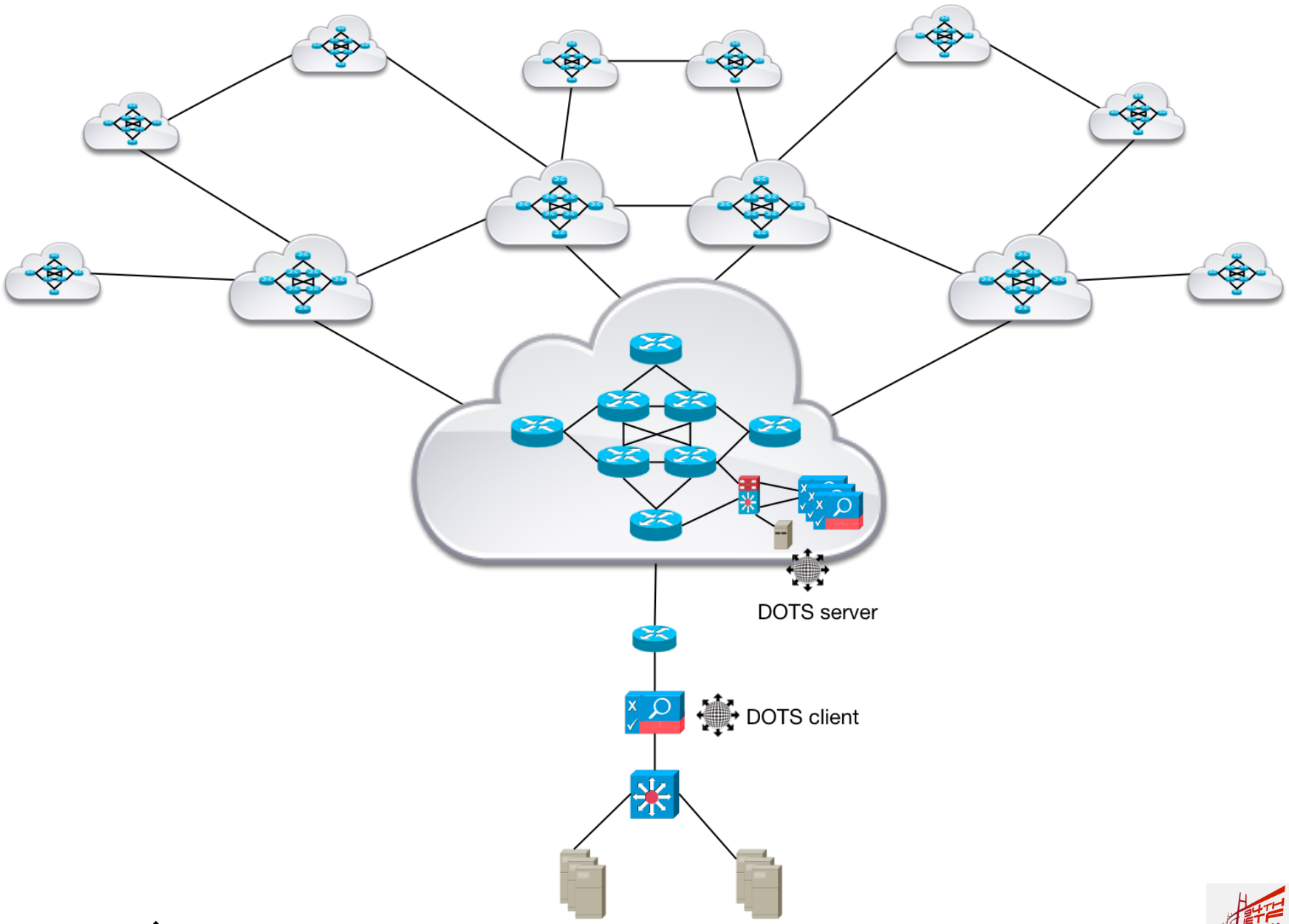
- 提供DOTS的示例用例（实际上是类别）。
- 所有示例可以是CE / PE或PE / PE。
- 每个类别的差异很大（请参阅4.1.1）。
- 每个示例中的所有DOTS通信都可以直接在DOTS服务器和DOTS客户端之间进行，也可以由DOTS中继进行协调。
- DOTS中继可以使用无状态传输，有状态传输或两者结合在DOTS客户端和服务器之间转发消息。
- DOTS中继可以聚合服务请求，状态消息和响应。
- DOTS中继可以过滤服务请求，状态消息和响应

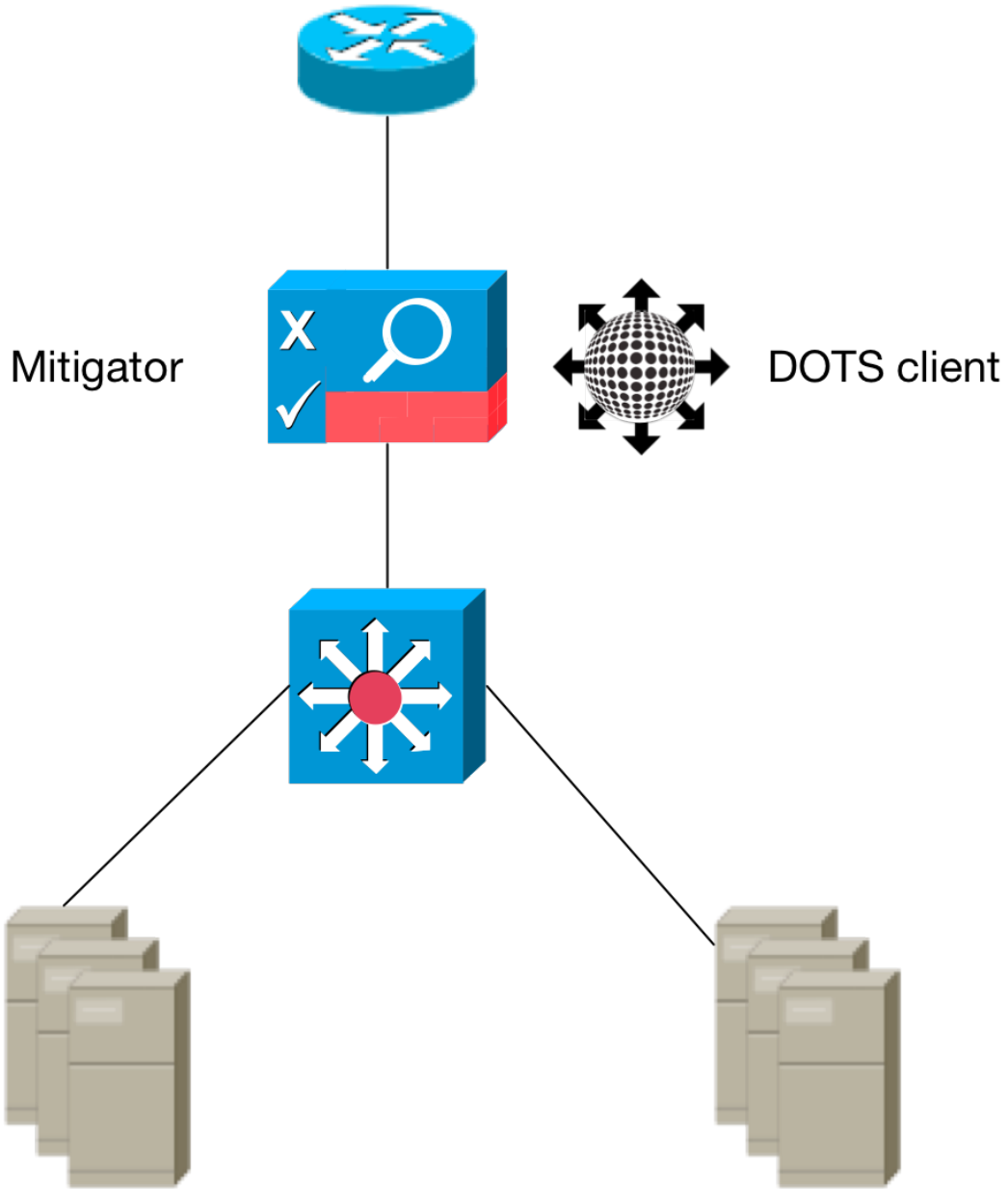
draft-ietf-dots-use-cases-00 摘要（续）

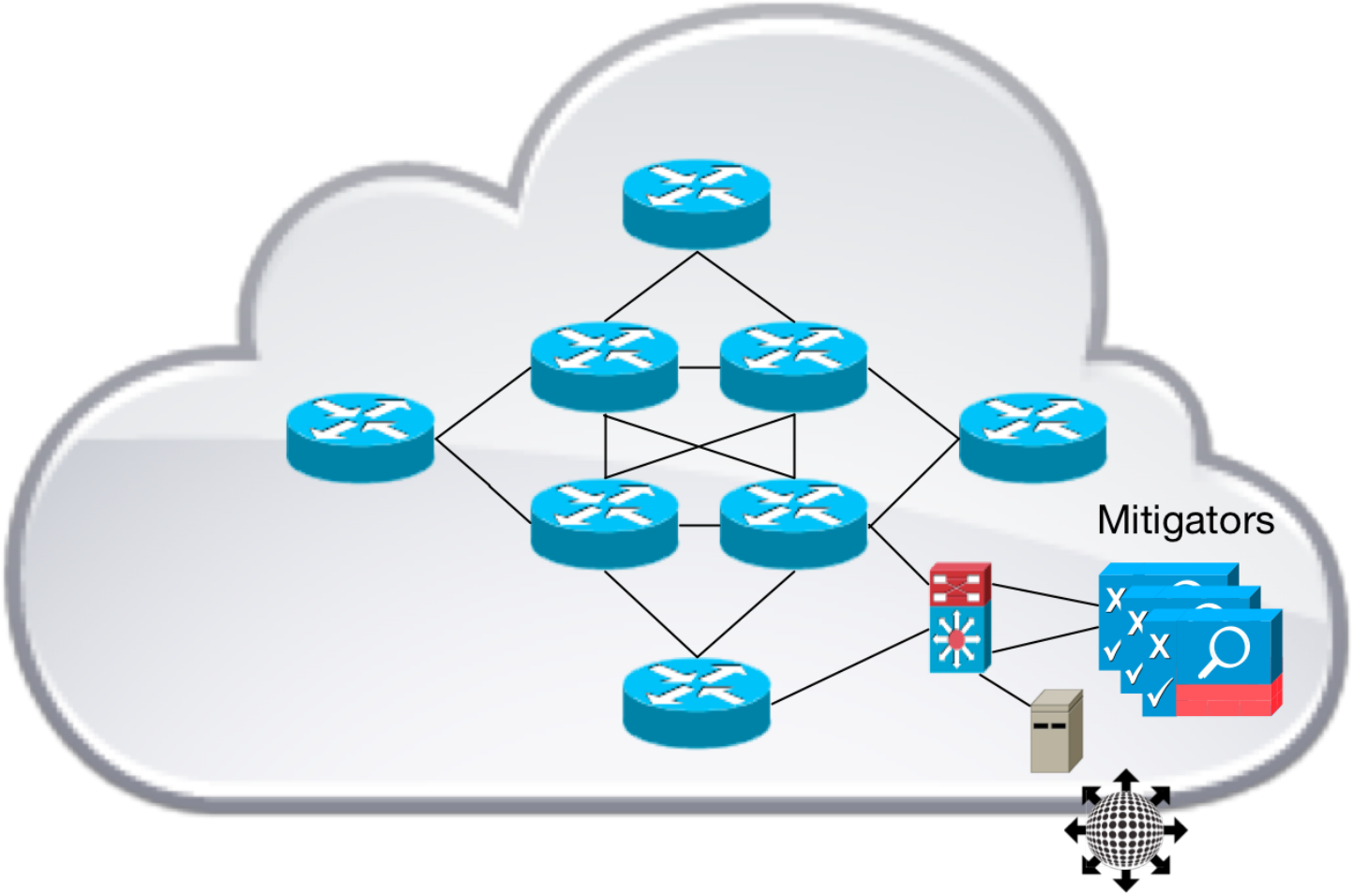
- -00中的用例并不详尽，仅用于说明。
- -00中的用例着重于使用专用缓解设备的分布式拒绝服务缓解 。S/ RTBH，flowspec，OpenFlow等也可用于利用网络基础设施进行分布式拒绝服务缓解。
- 本演示文稿中的4.1.1用例说明了完整的DOTS通信周期及其变体。
- 本演示文稿中的其他用例总结为“差异”，说明了在多种不同情况下的DOTS通信模型。
- 本演示中的用例侧重于保护目标网络受到分布式拒绝服务攻击时的服务器。DOTS还可以用于抑制原始网络或穿越中间网

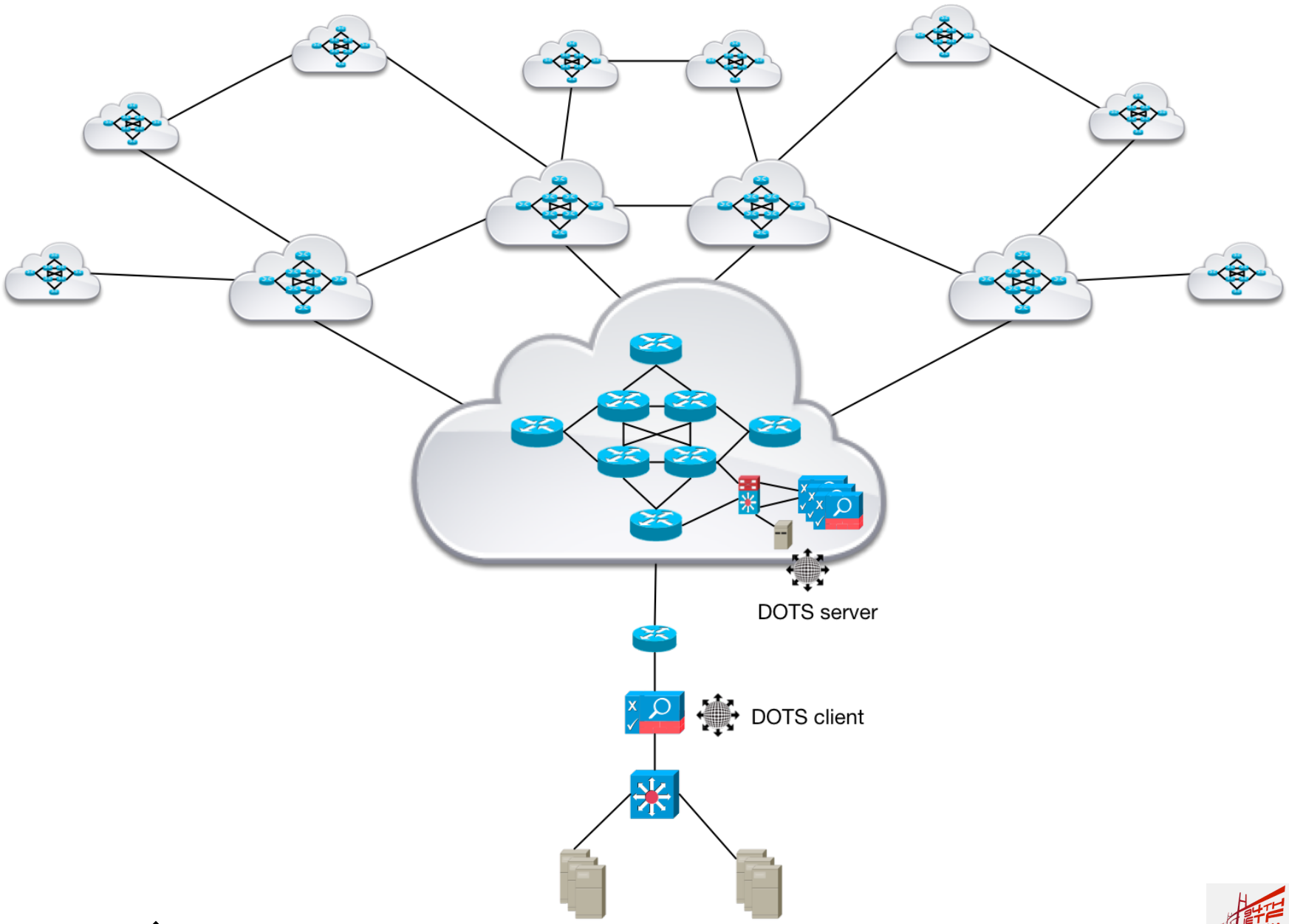
4.1-主要用例

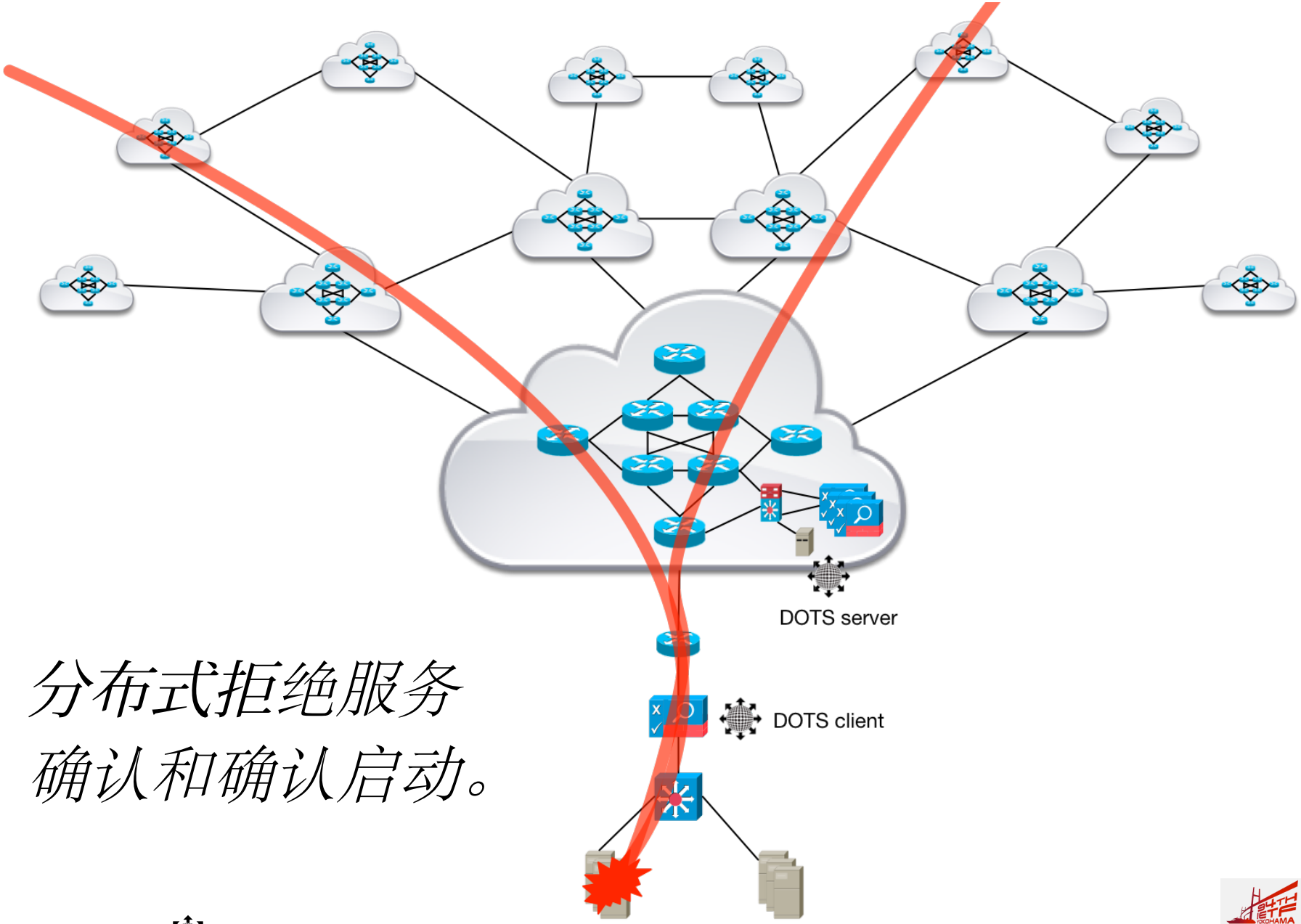
4.1.1 – CPE或PE缓解器请求上游分布式拒绝服务缓解


DOTS server
DOTS client


Mitigator
DOTS client

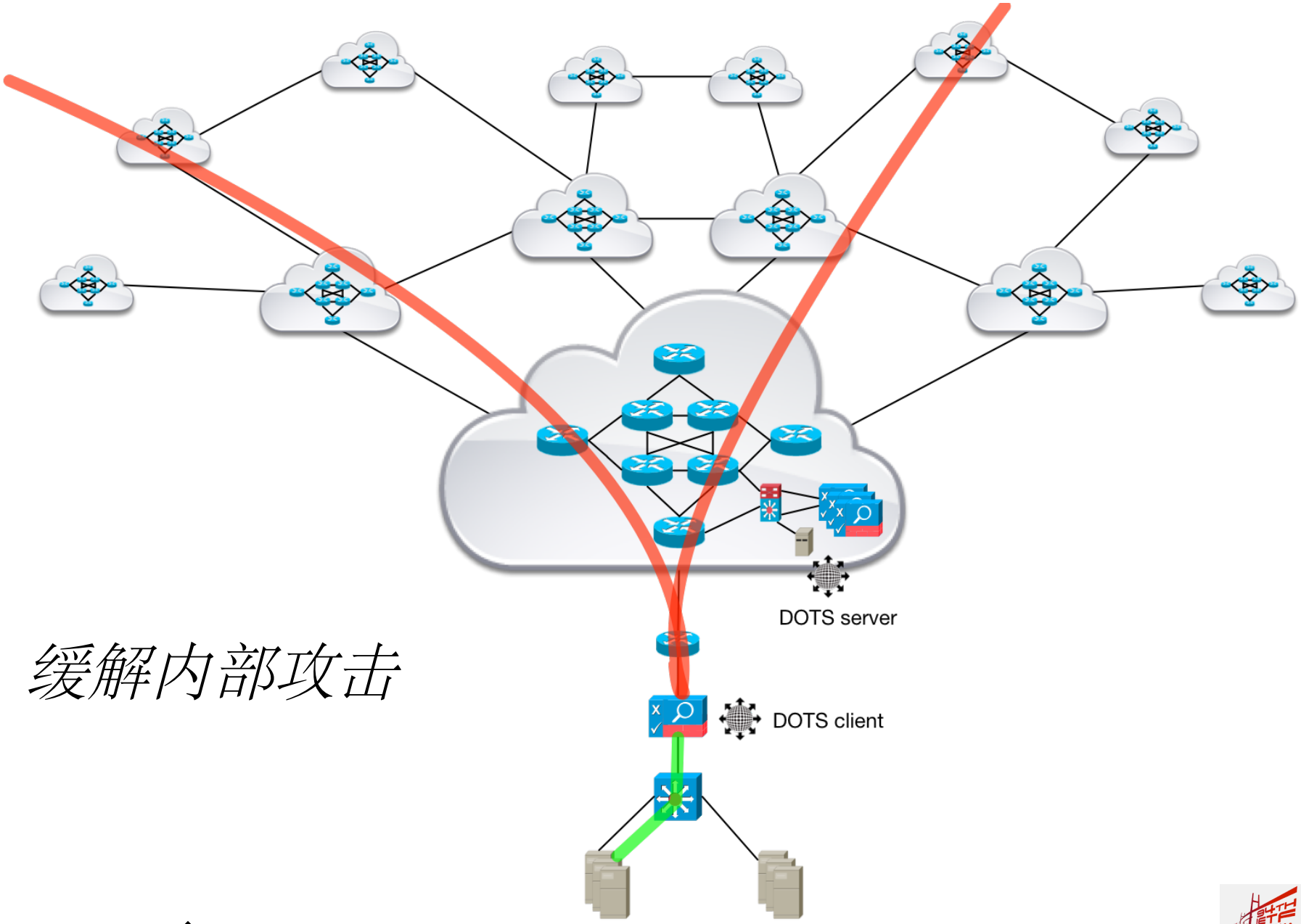

Mitigators
DOTS server


DOTS server
DOTS client

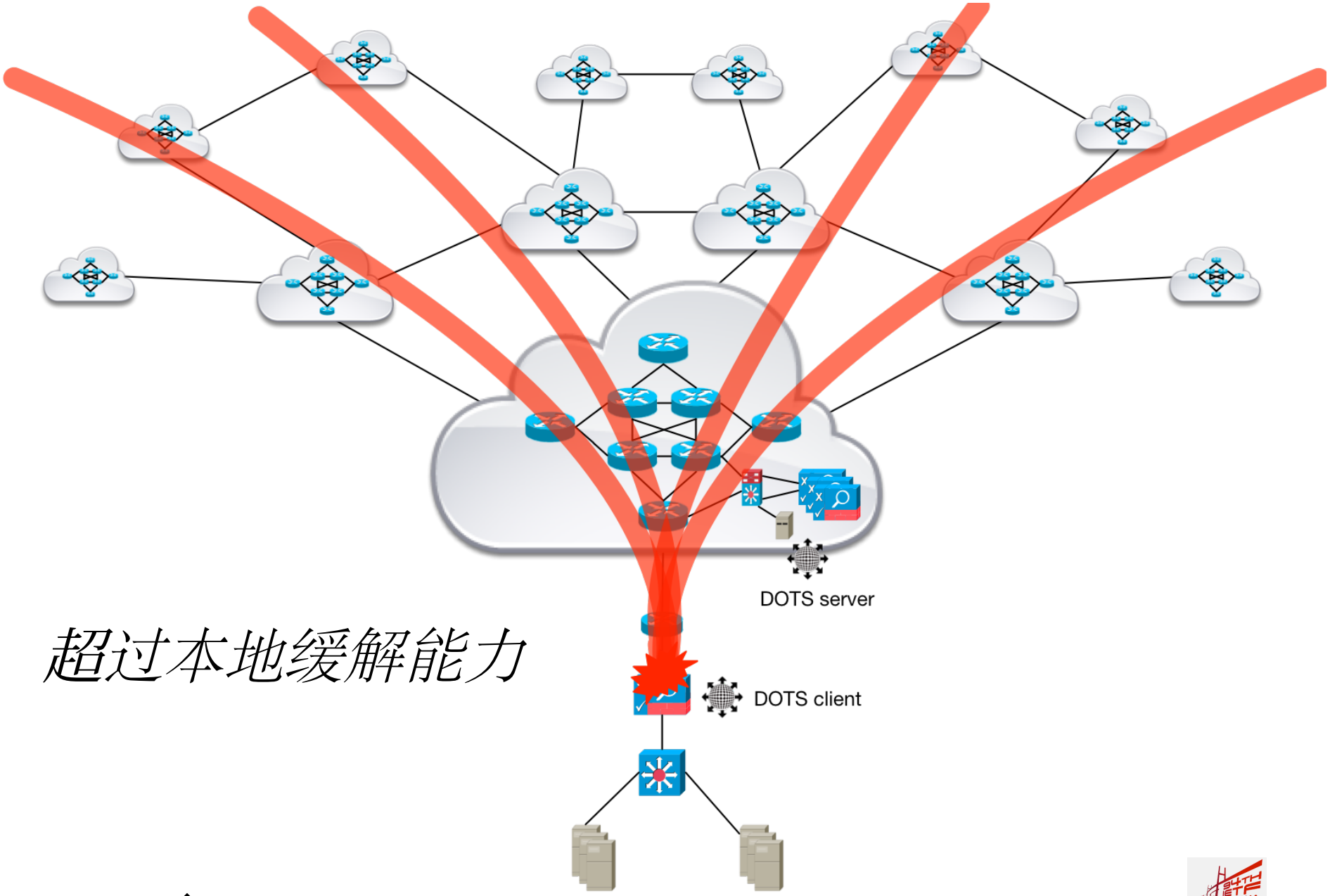


分布式拒绝服务
确认和确认启动。

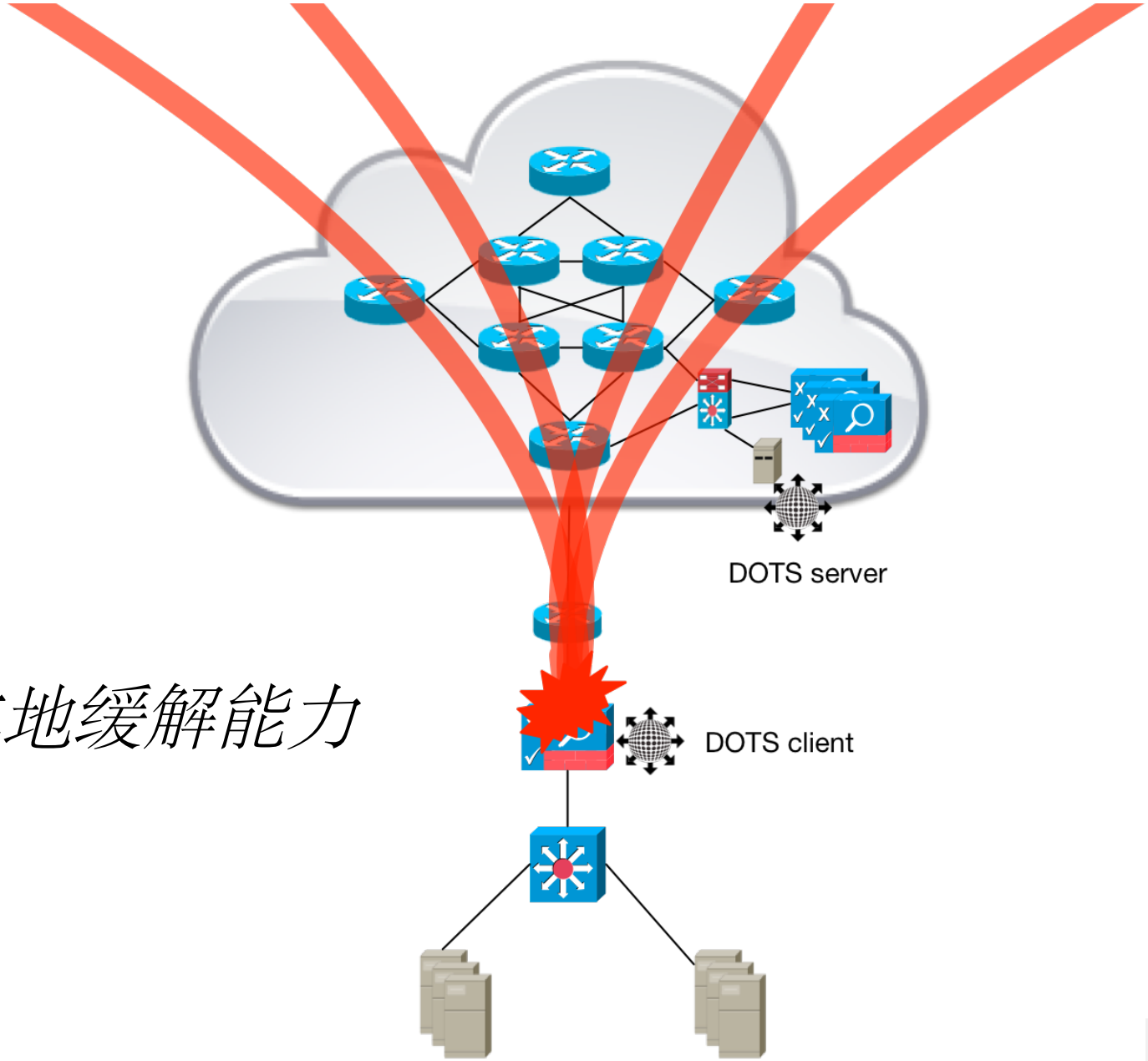
缓解内部攻击

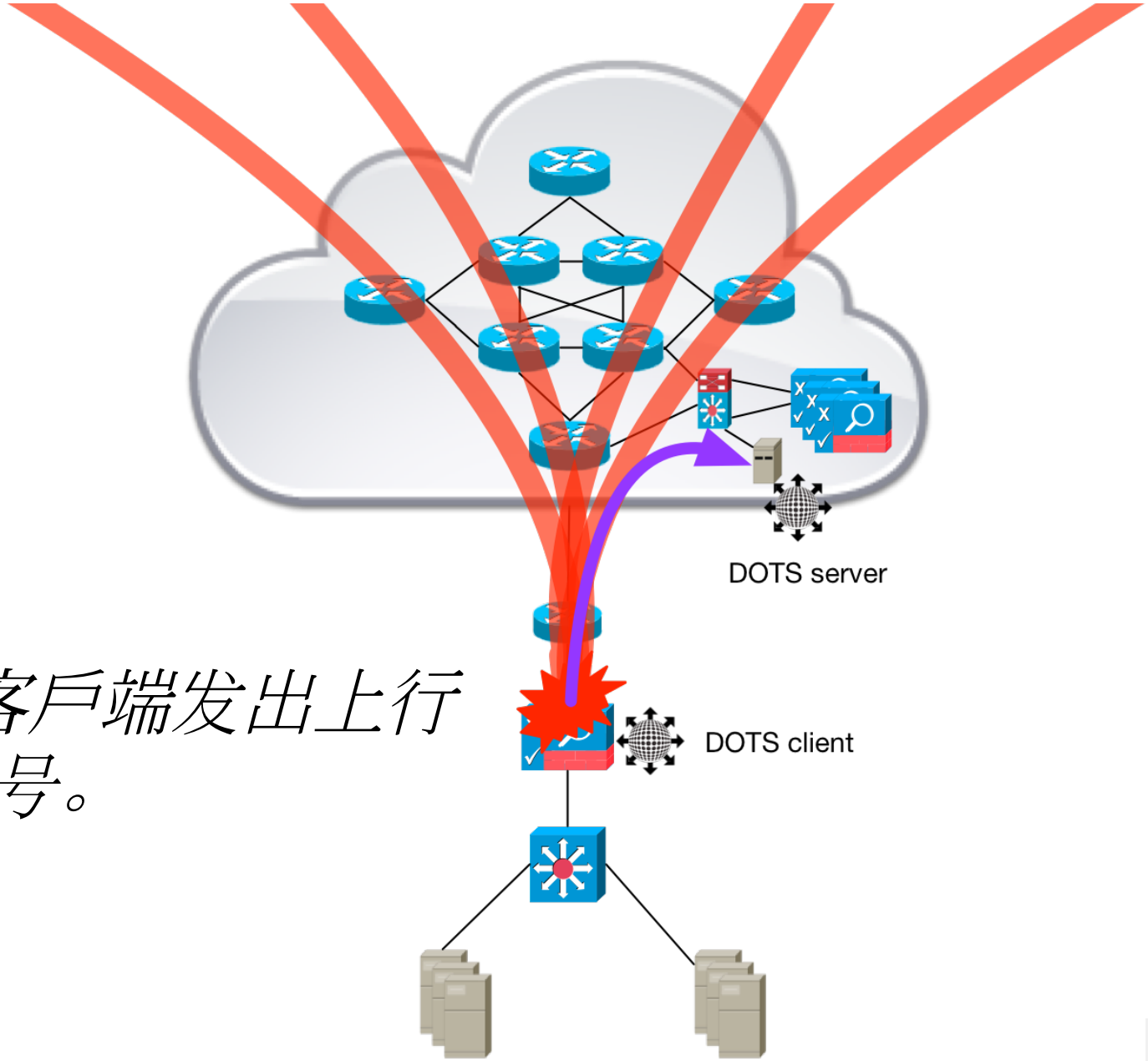


超过本地缓解能力

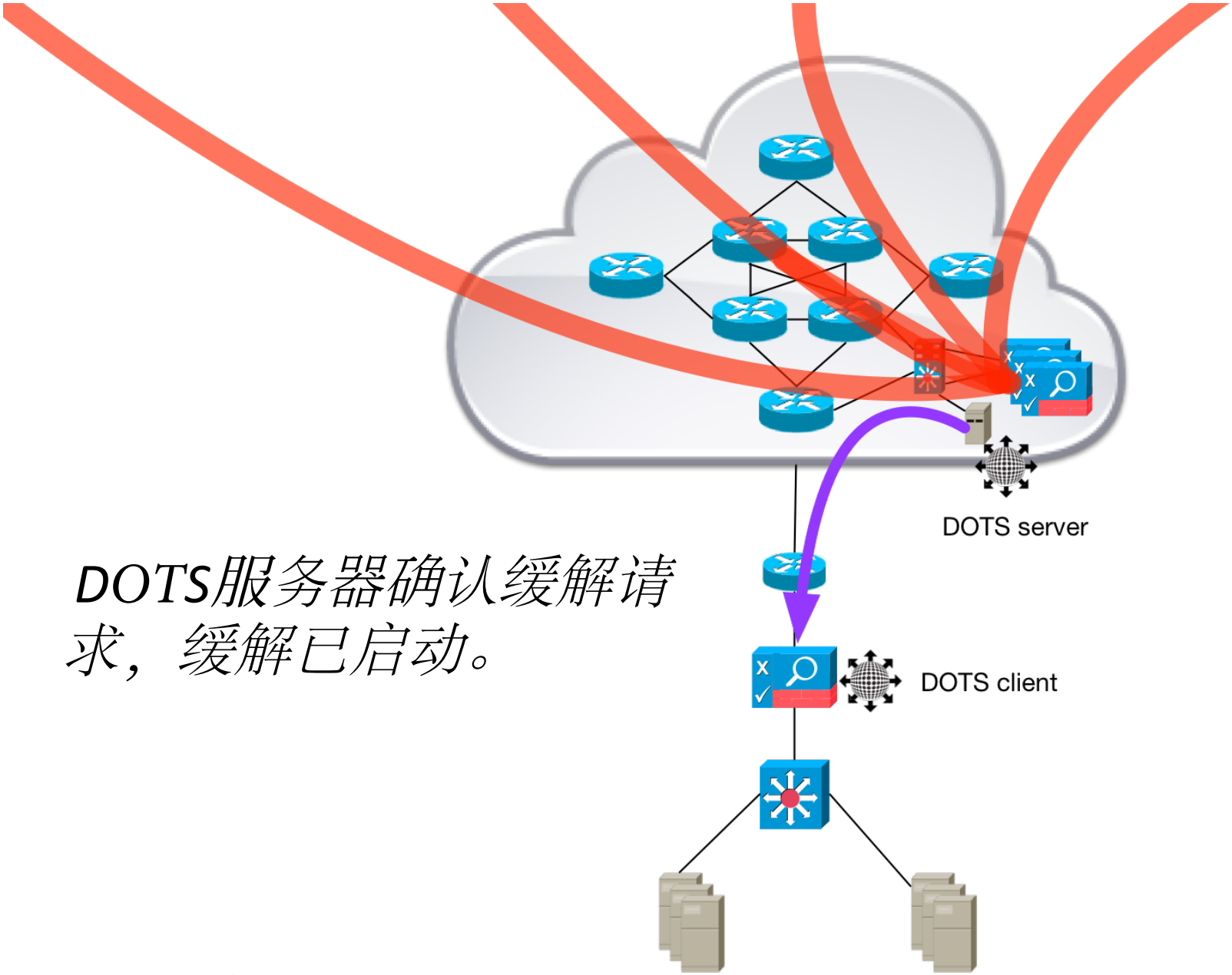


超过本地缓解能力



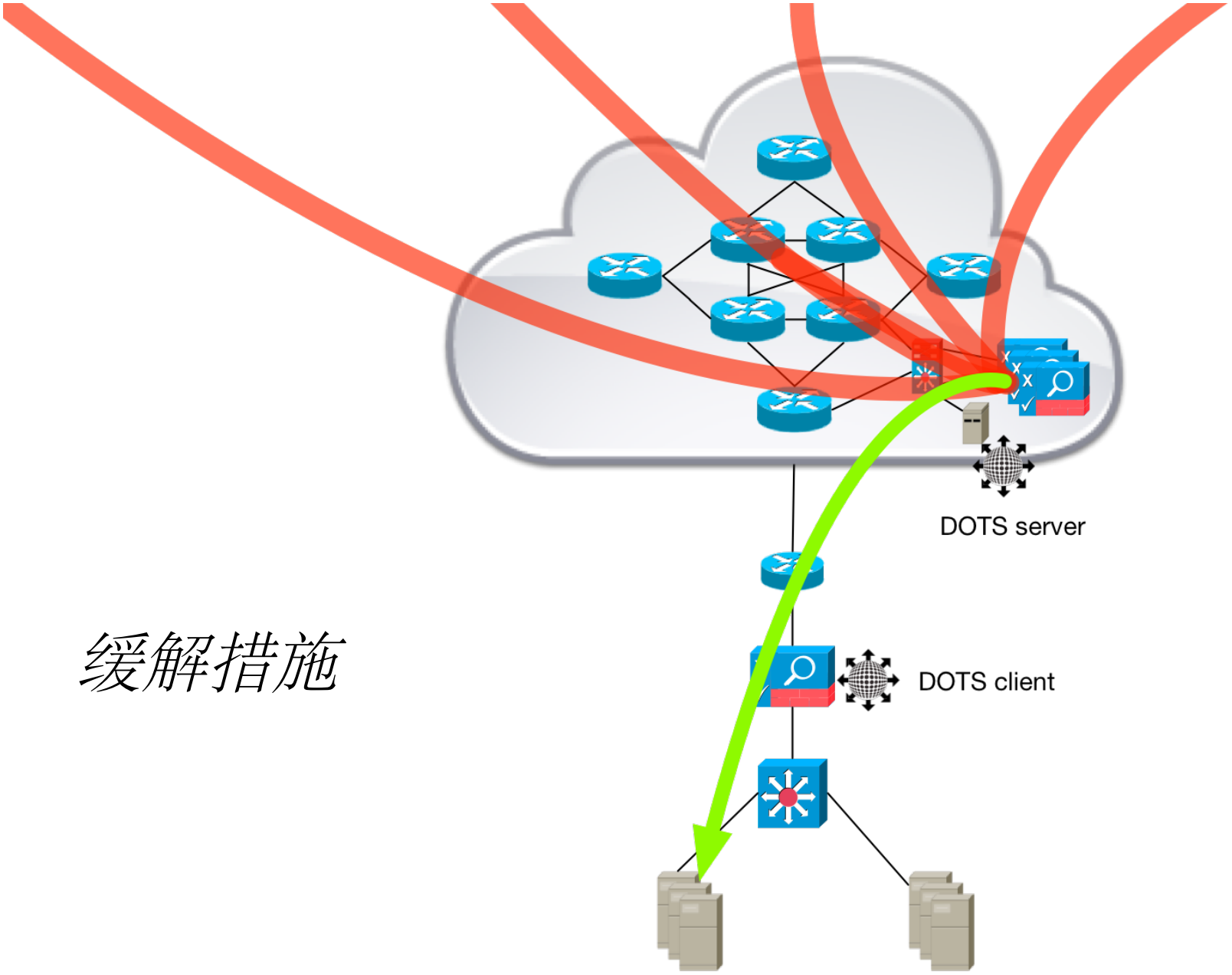


DOTS客戶端发出上行缓解信号。

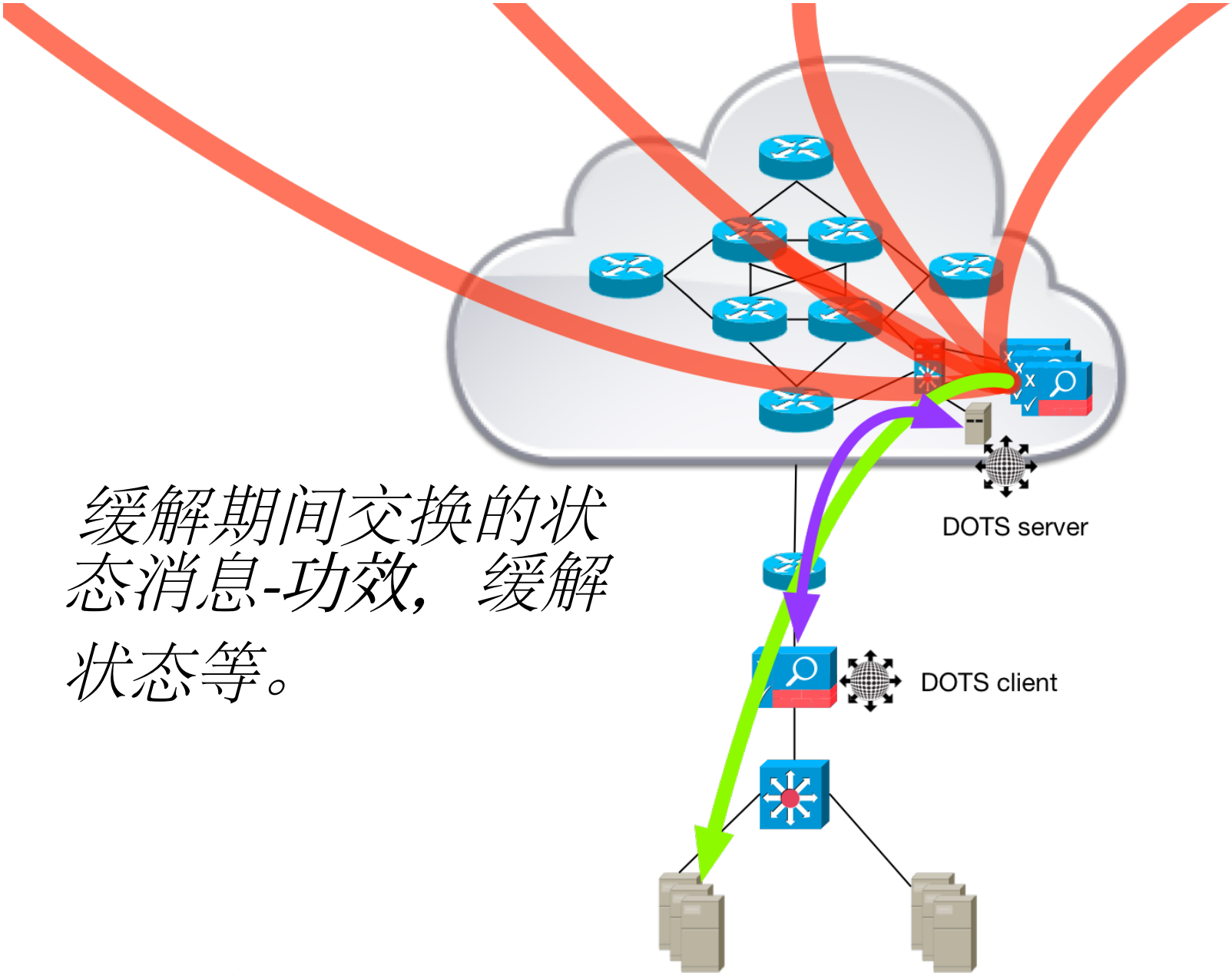


DOTS服务器确认缓解请求，缓解已启动。

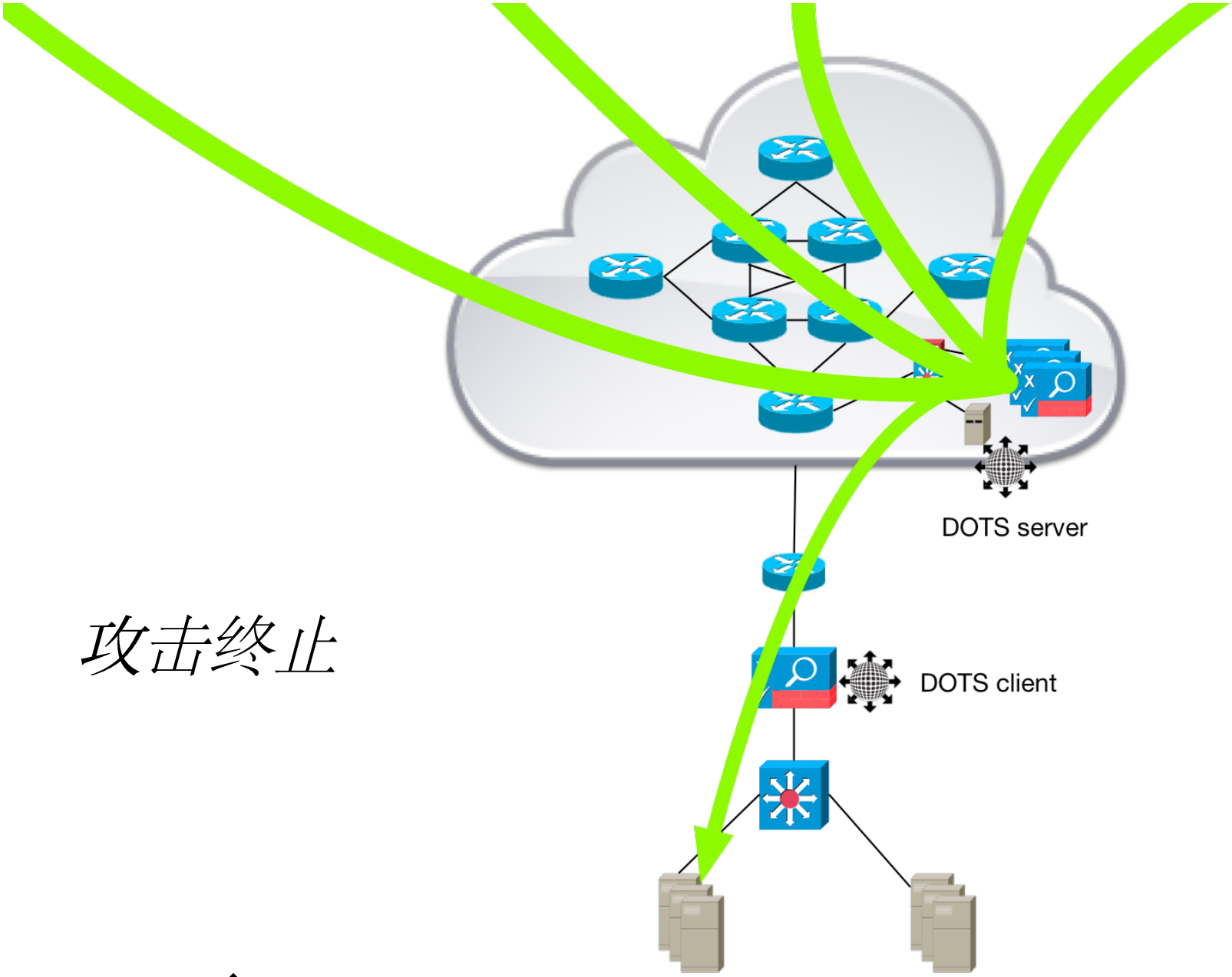
缓解措施

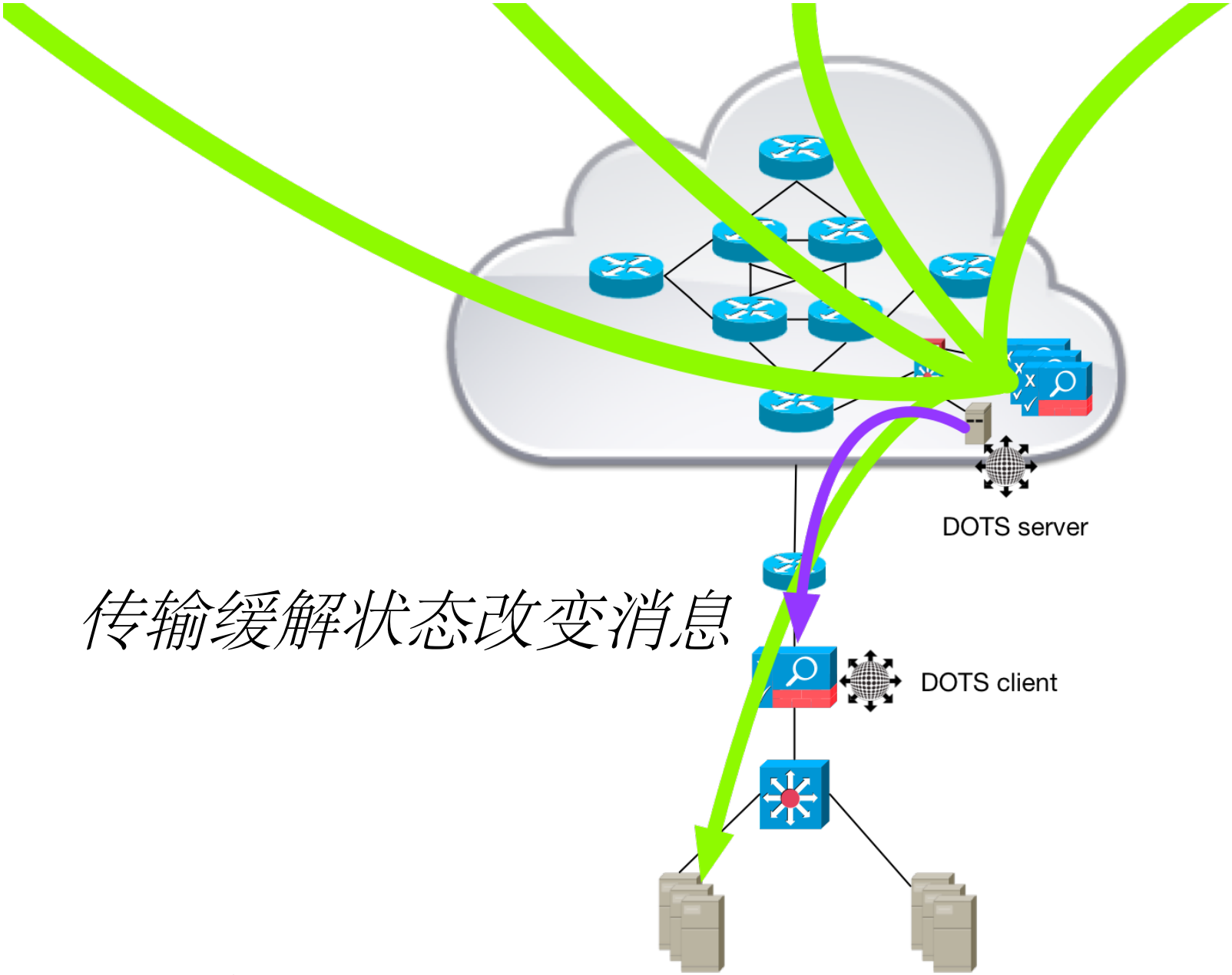


缓解期间交换的状态消息-功效，缓解状态等。



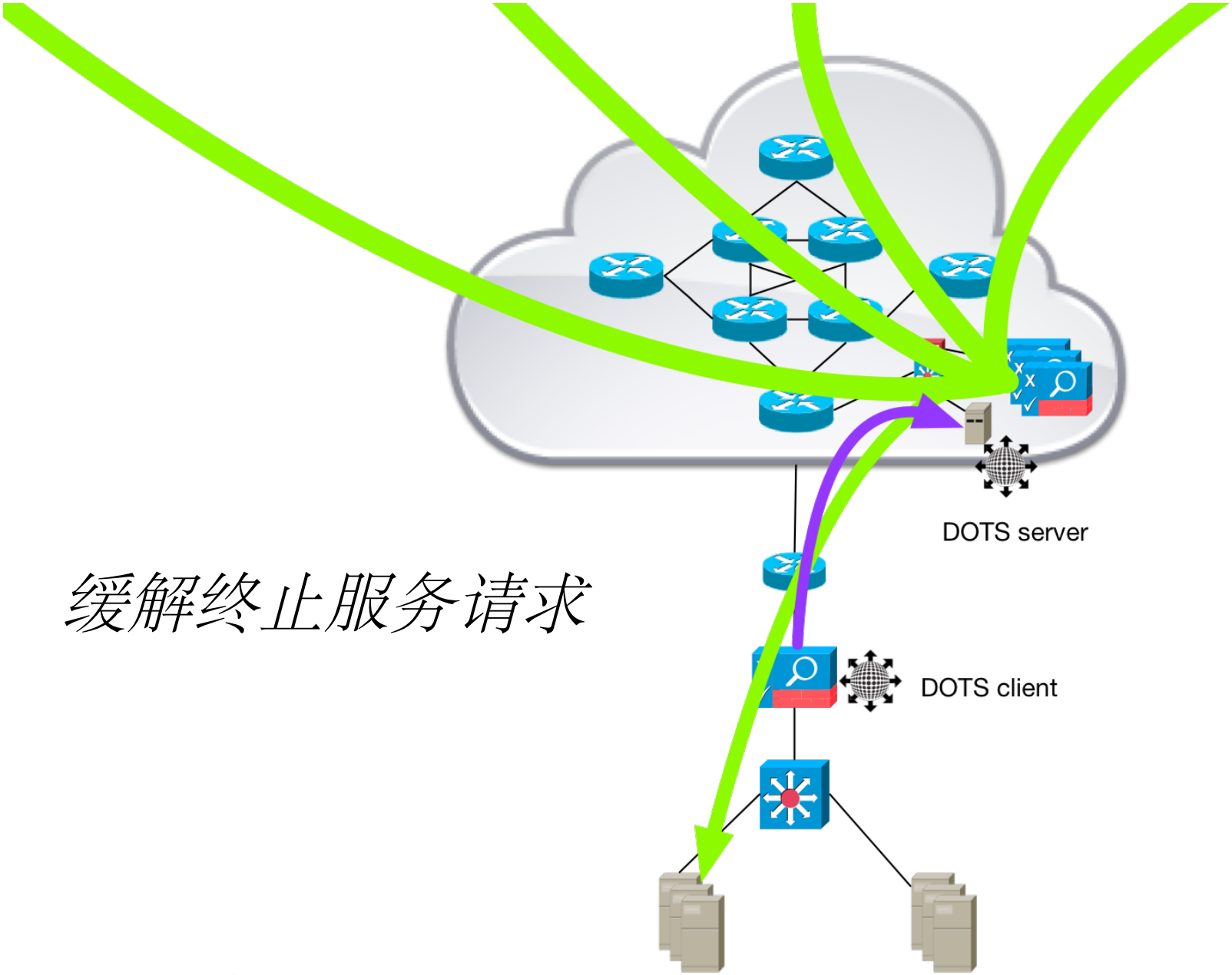
攻击终止



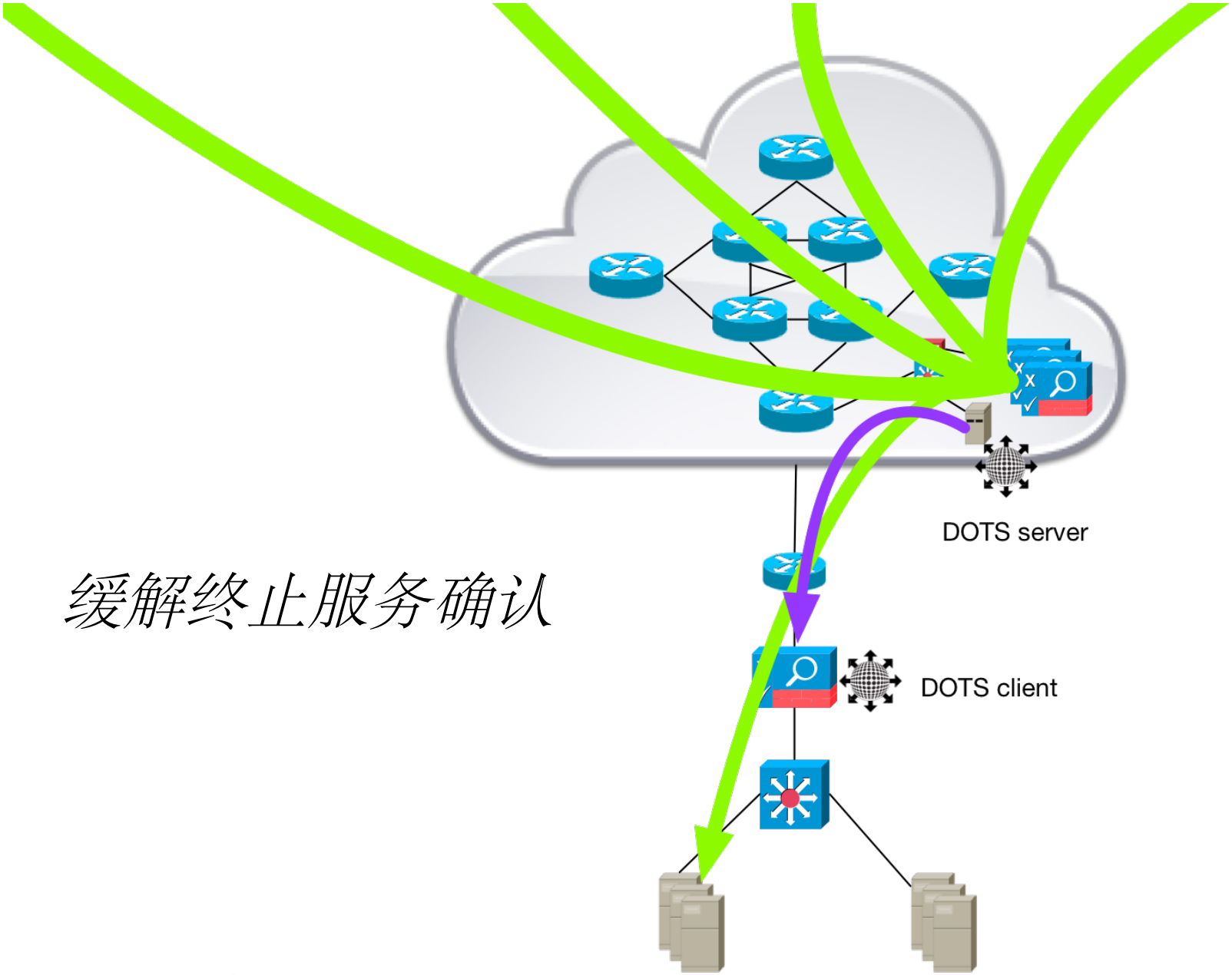


传输缓解状态改变消息

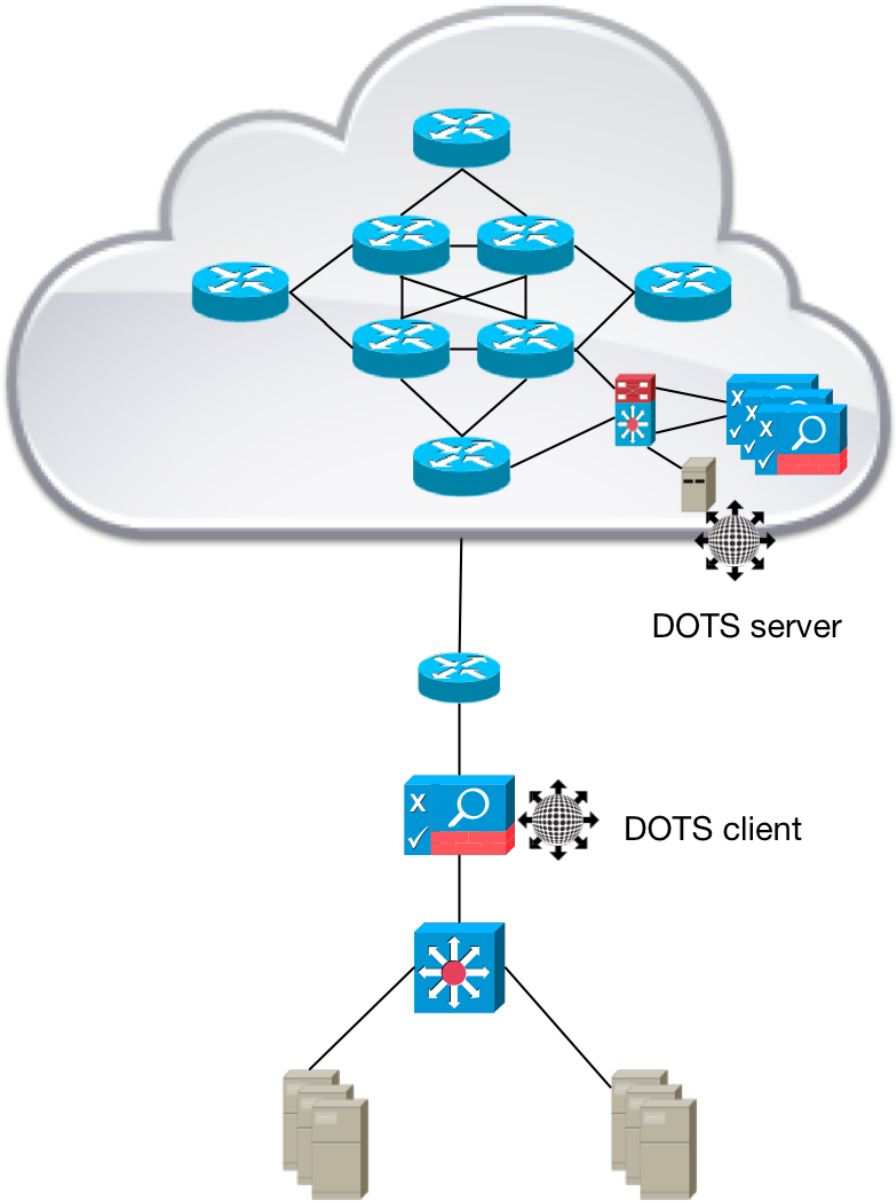
缓解终止服务请求



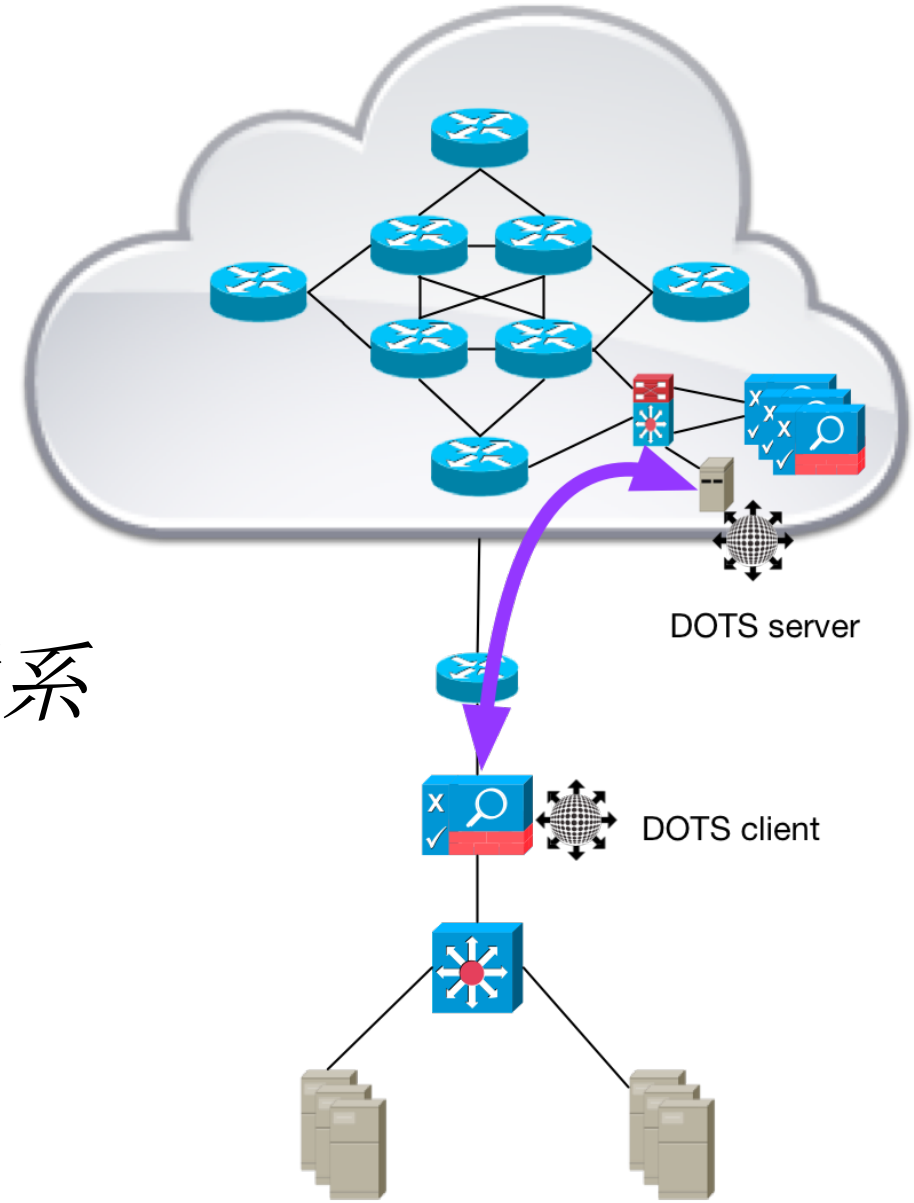
缓解终止服务确认



缓解已终止

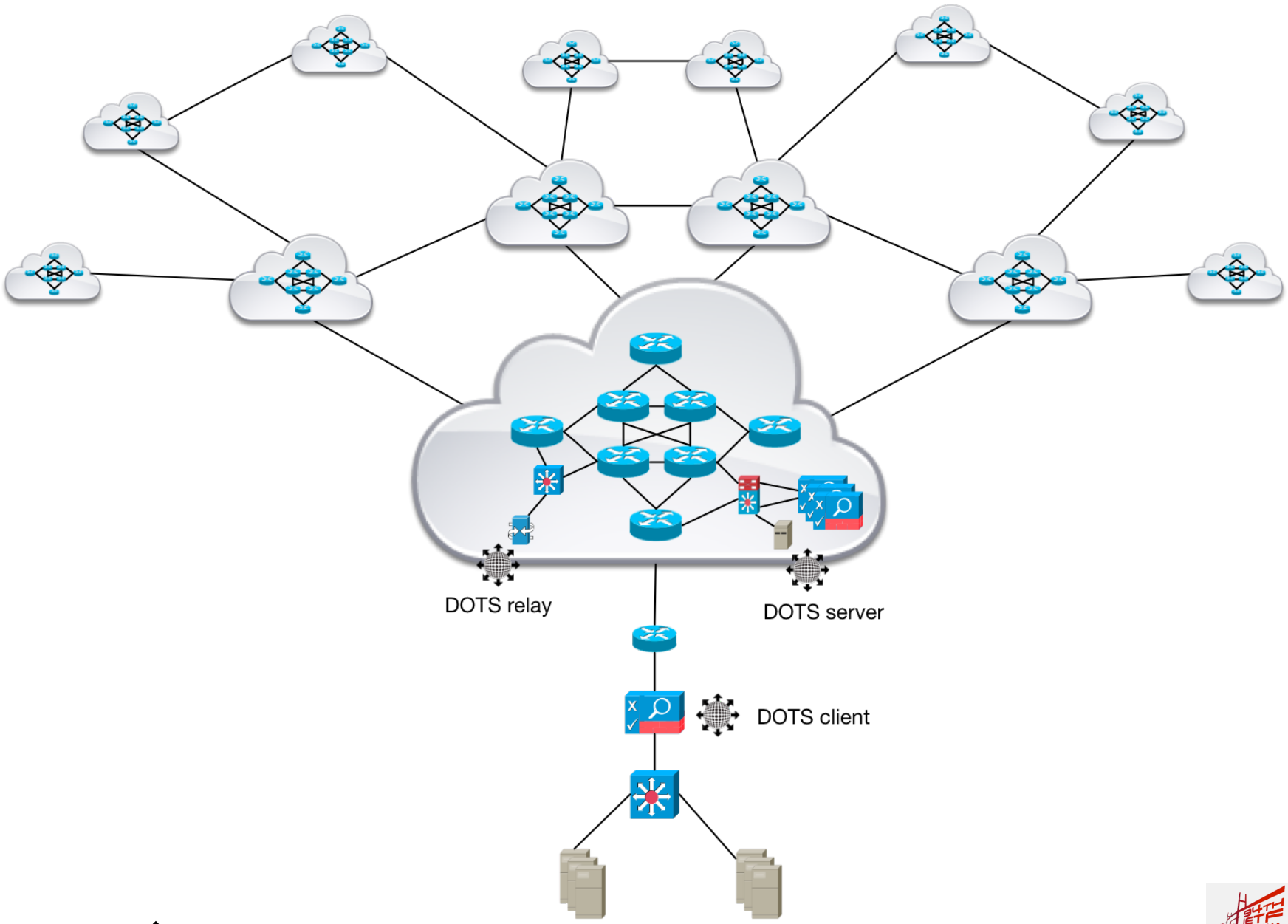


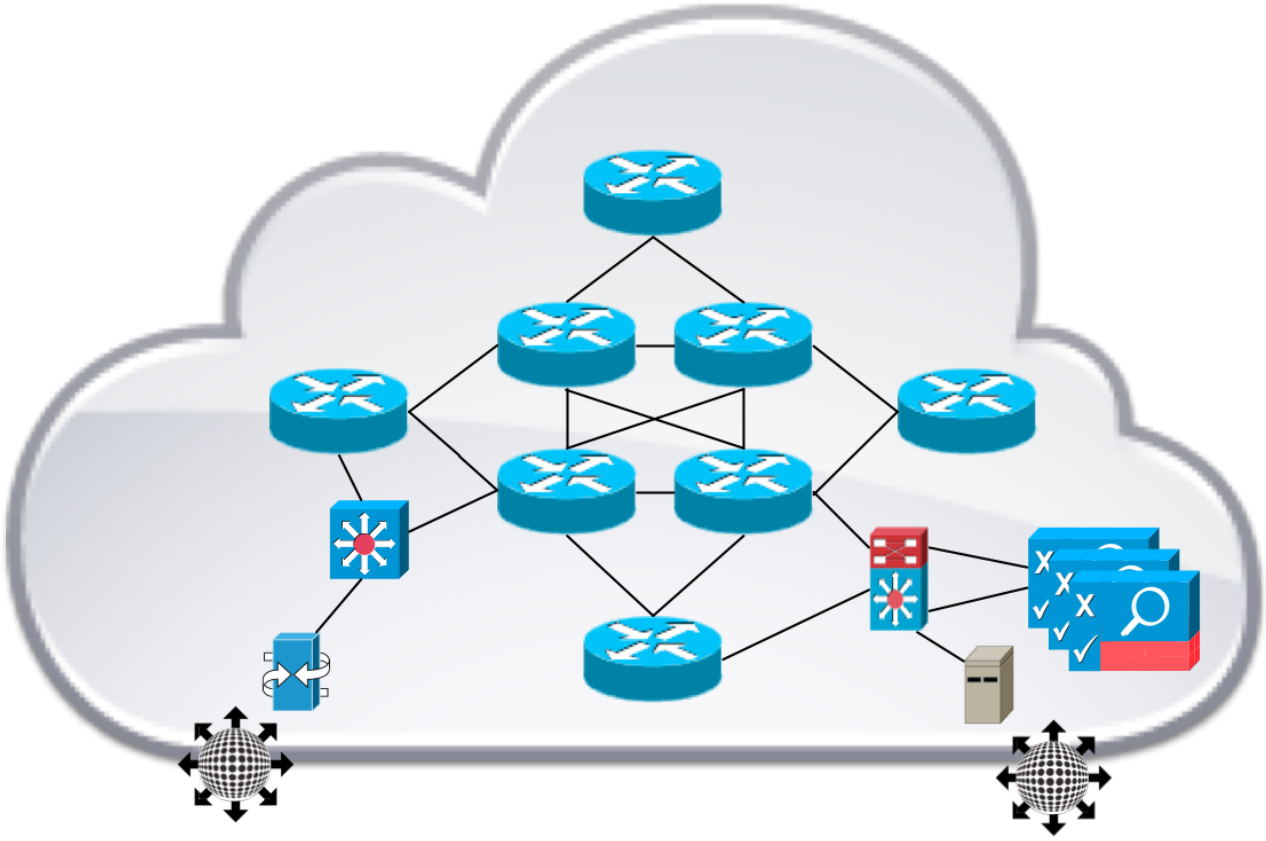
DOTS通信关系



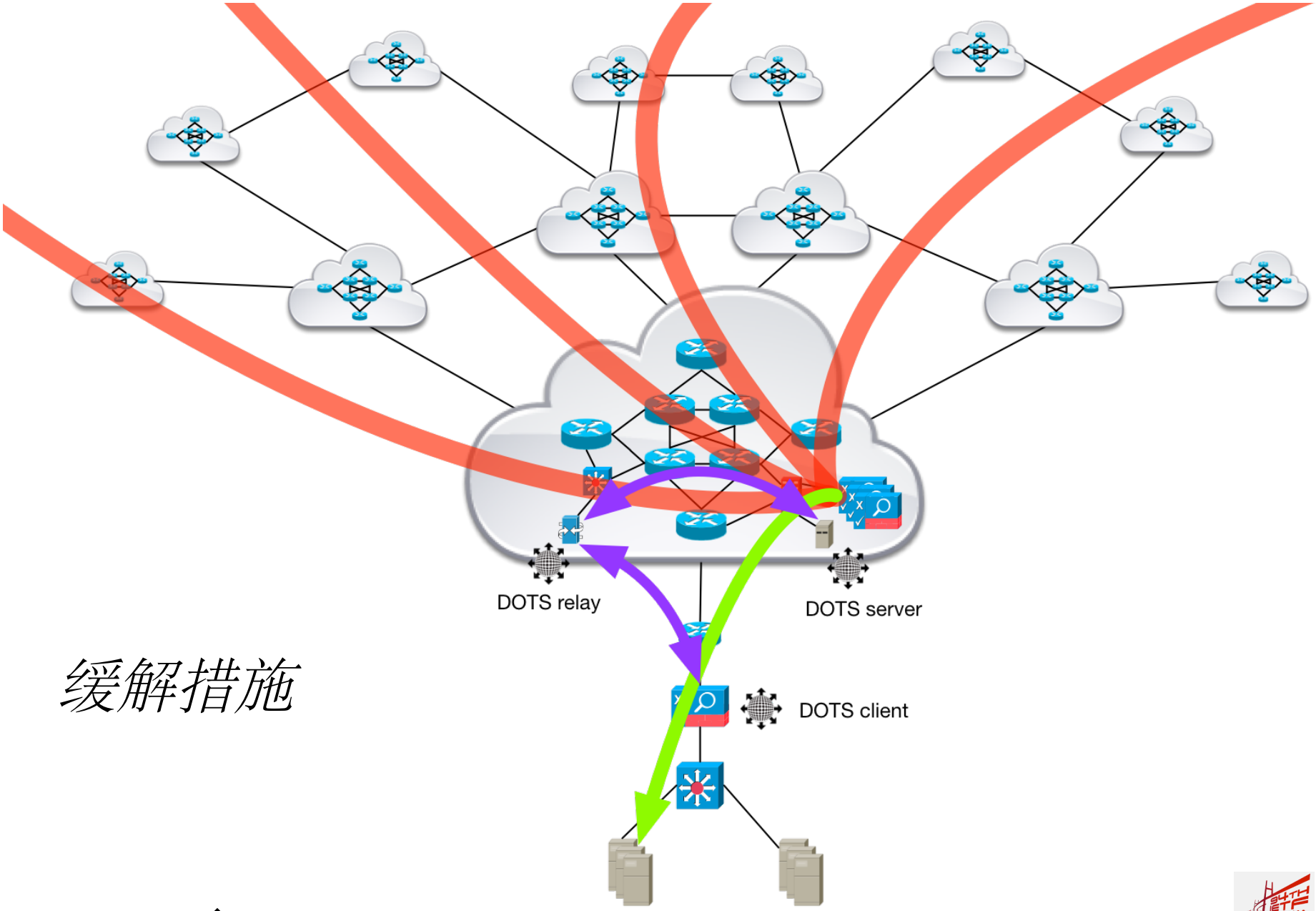
4.1.1 – 覆盖分布式拒绝服务的变化

缓解服务提供商

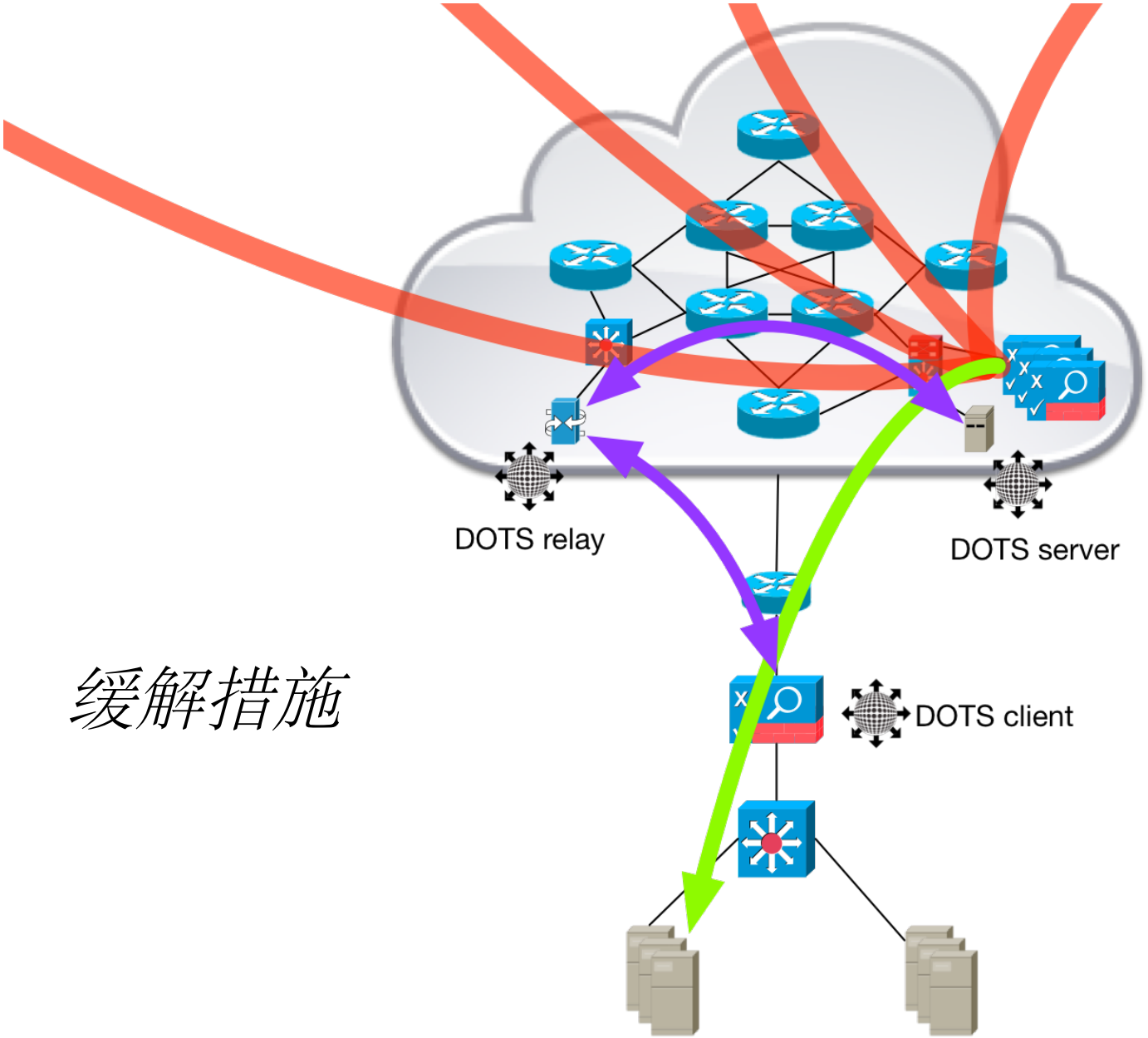

DOTS relay
DOTS server
DOTS client


DOTS relay
DOTS server

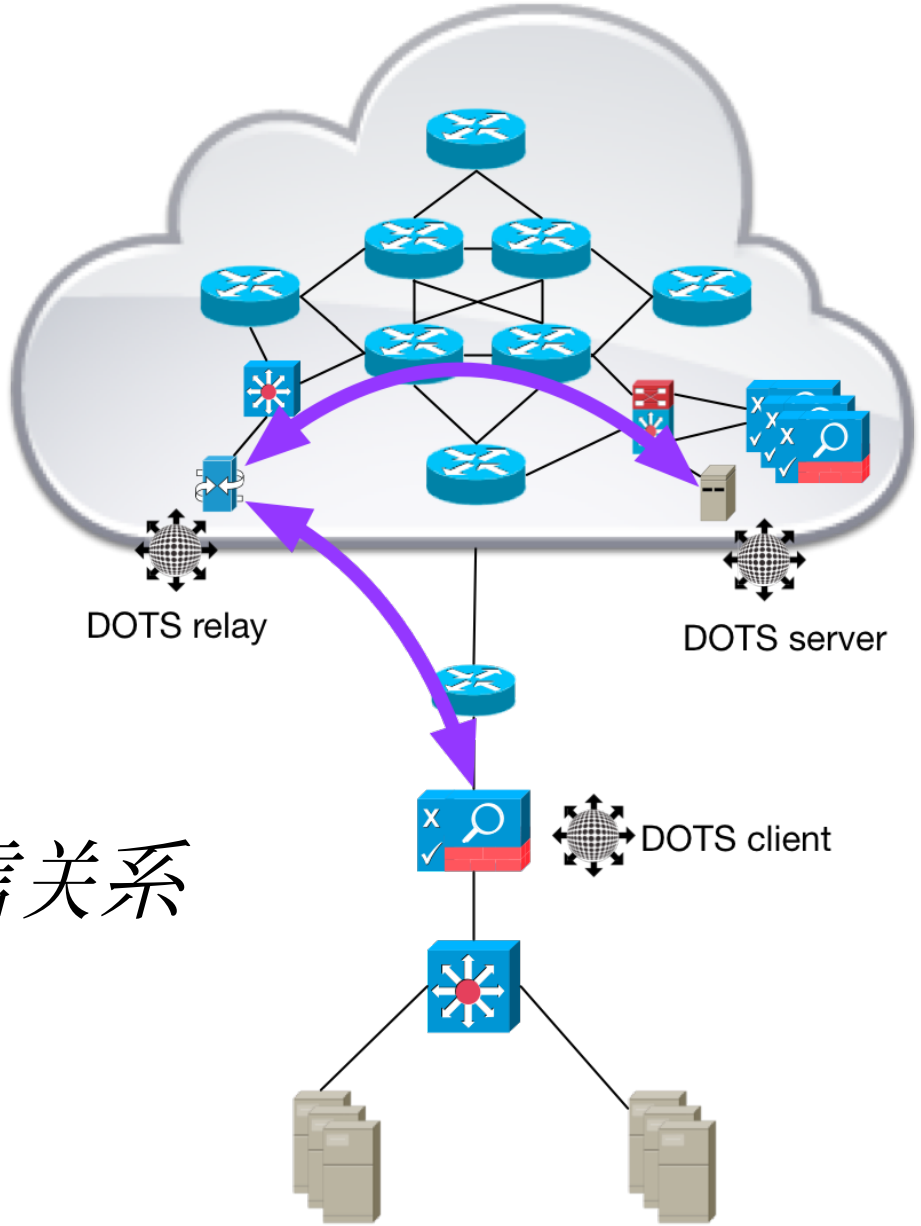
缓解措施



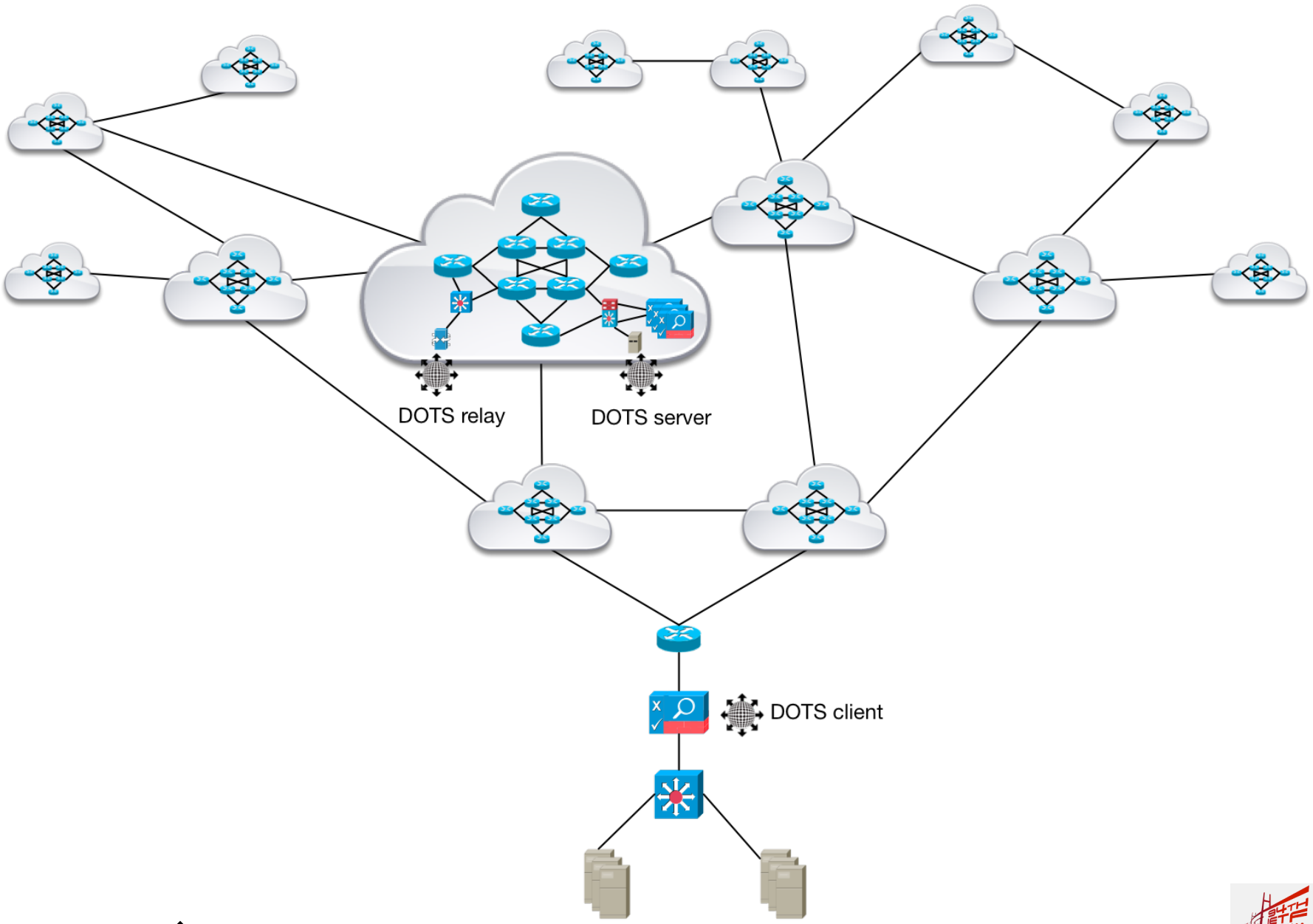
缓解措施



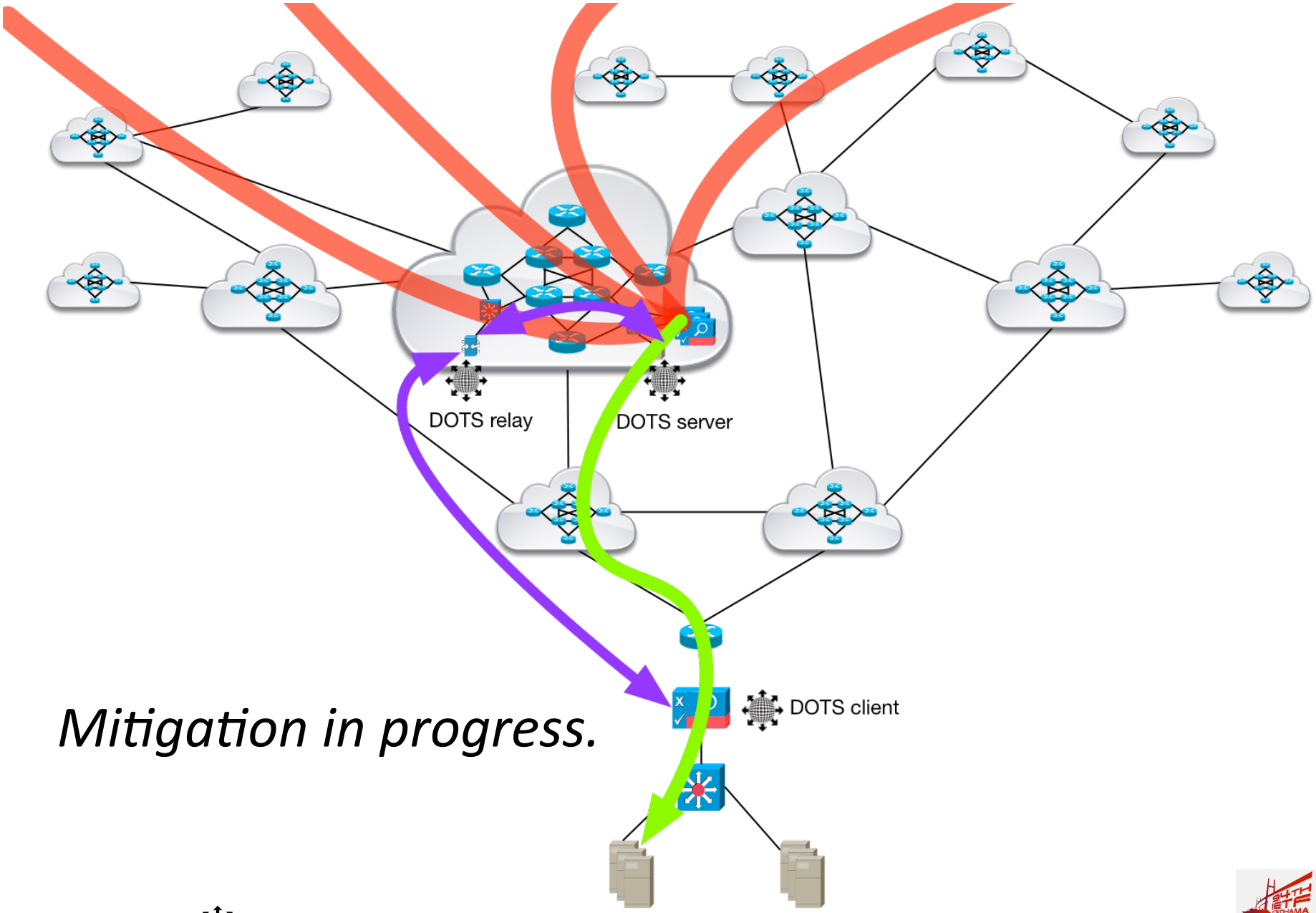
DOTS通信关系



4.1.1 – Variation with Overlay DDoS Mitigation Service Provider

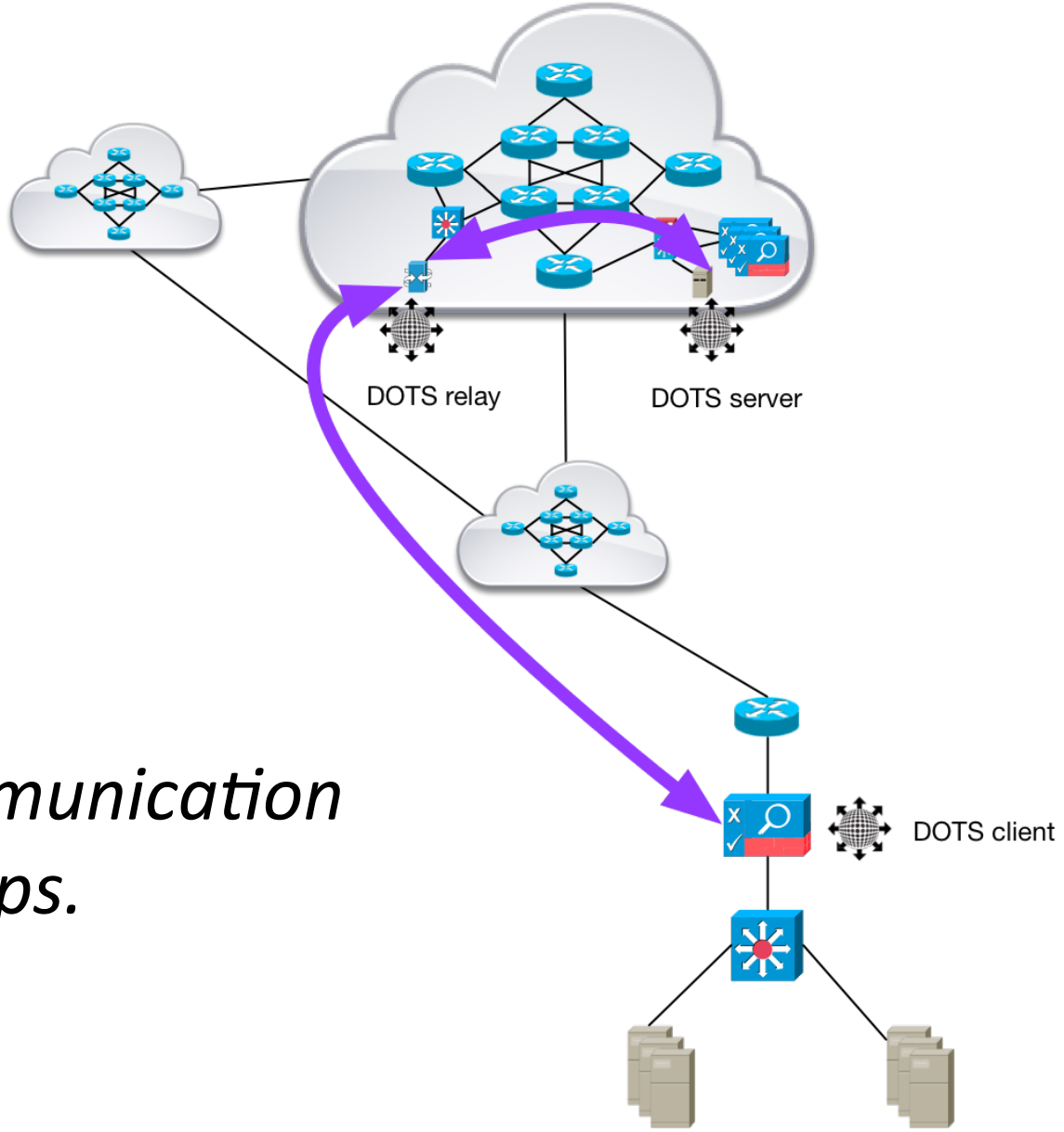


DOTS WG

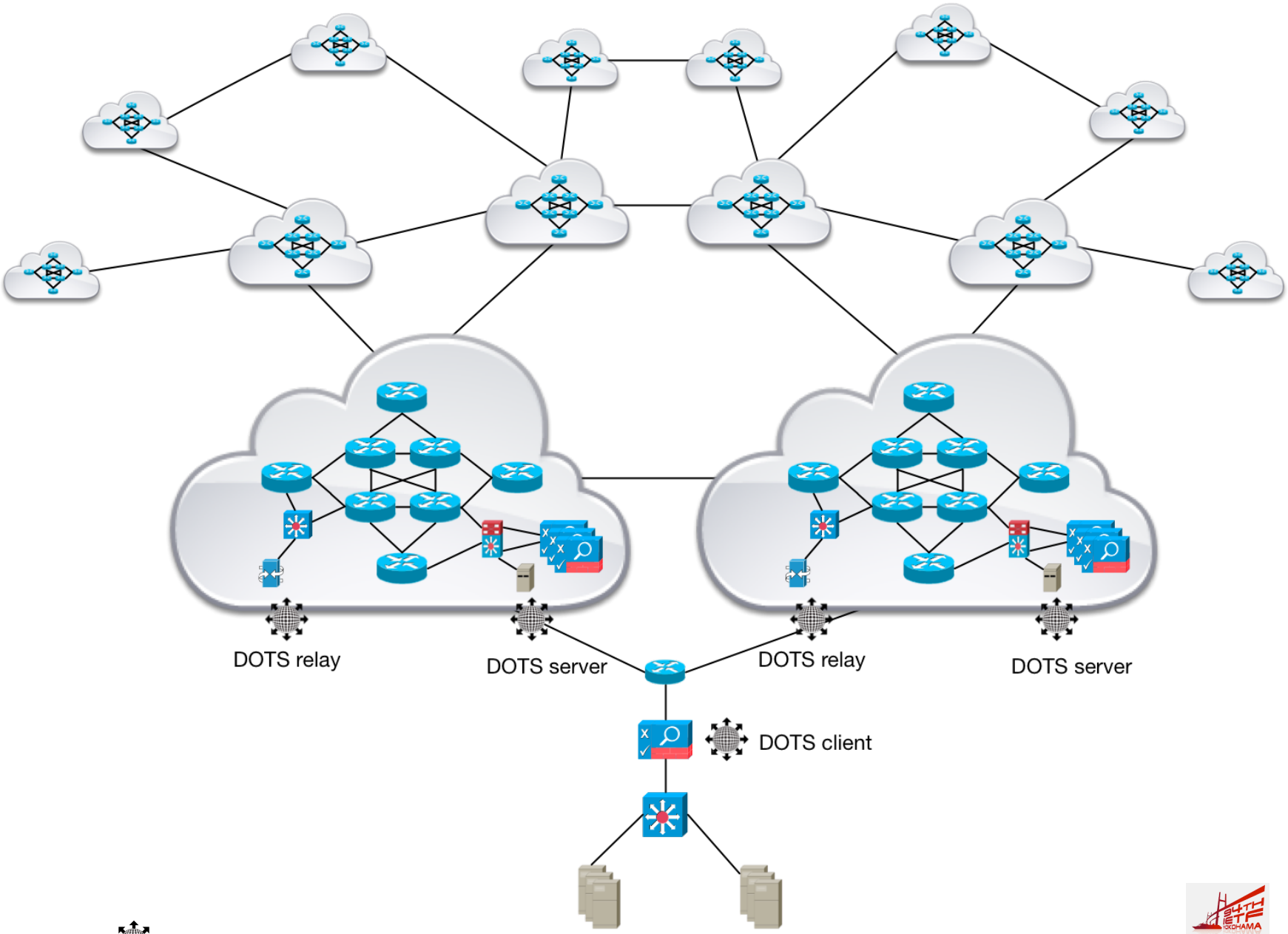


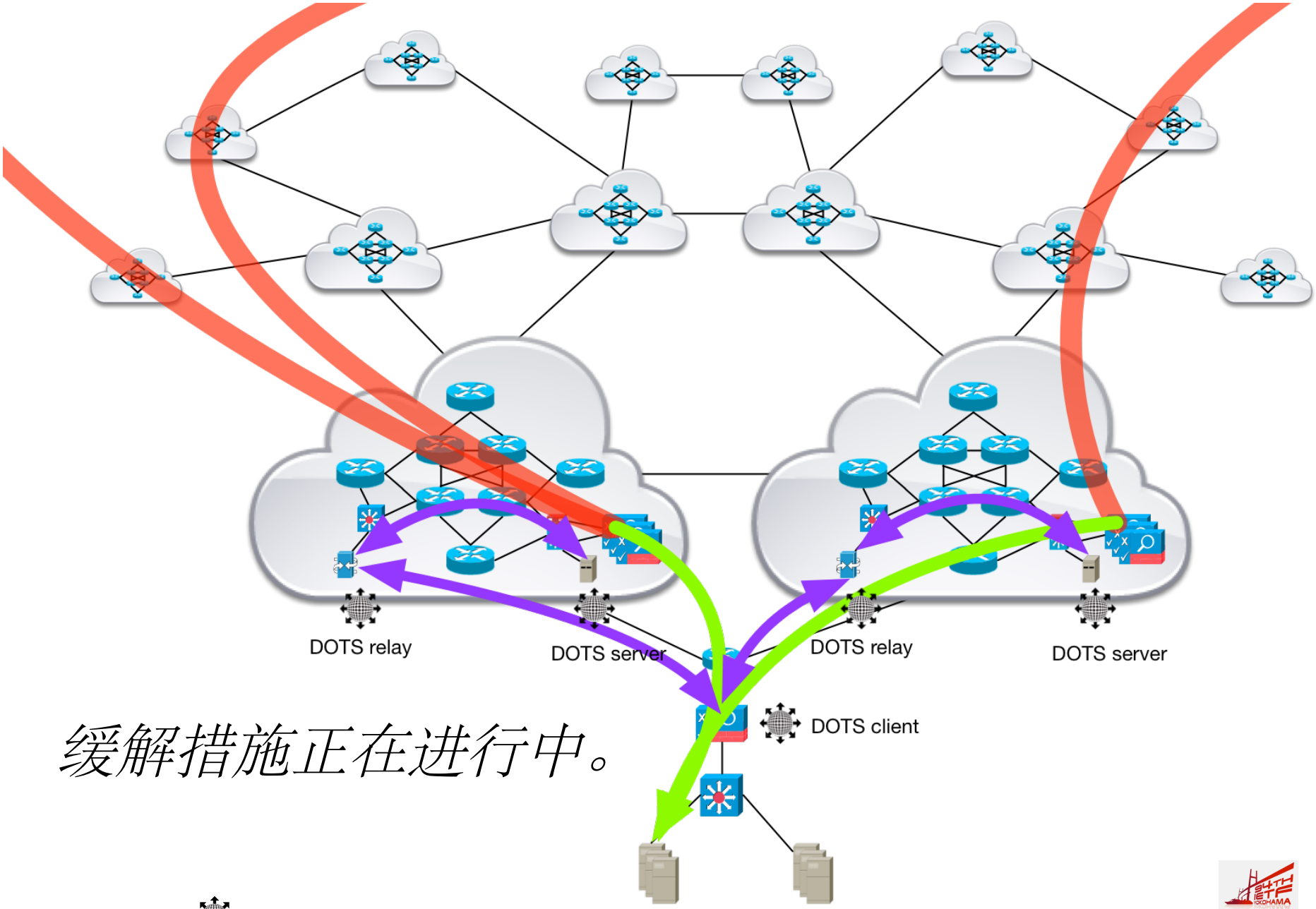
Mitigation in progress.

DOTS communication relationships.

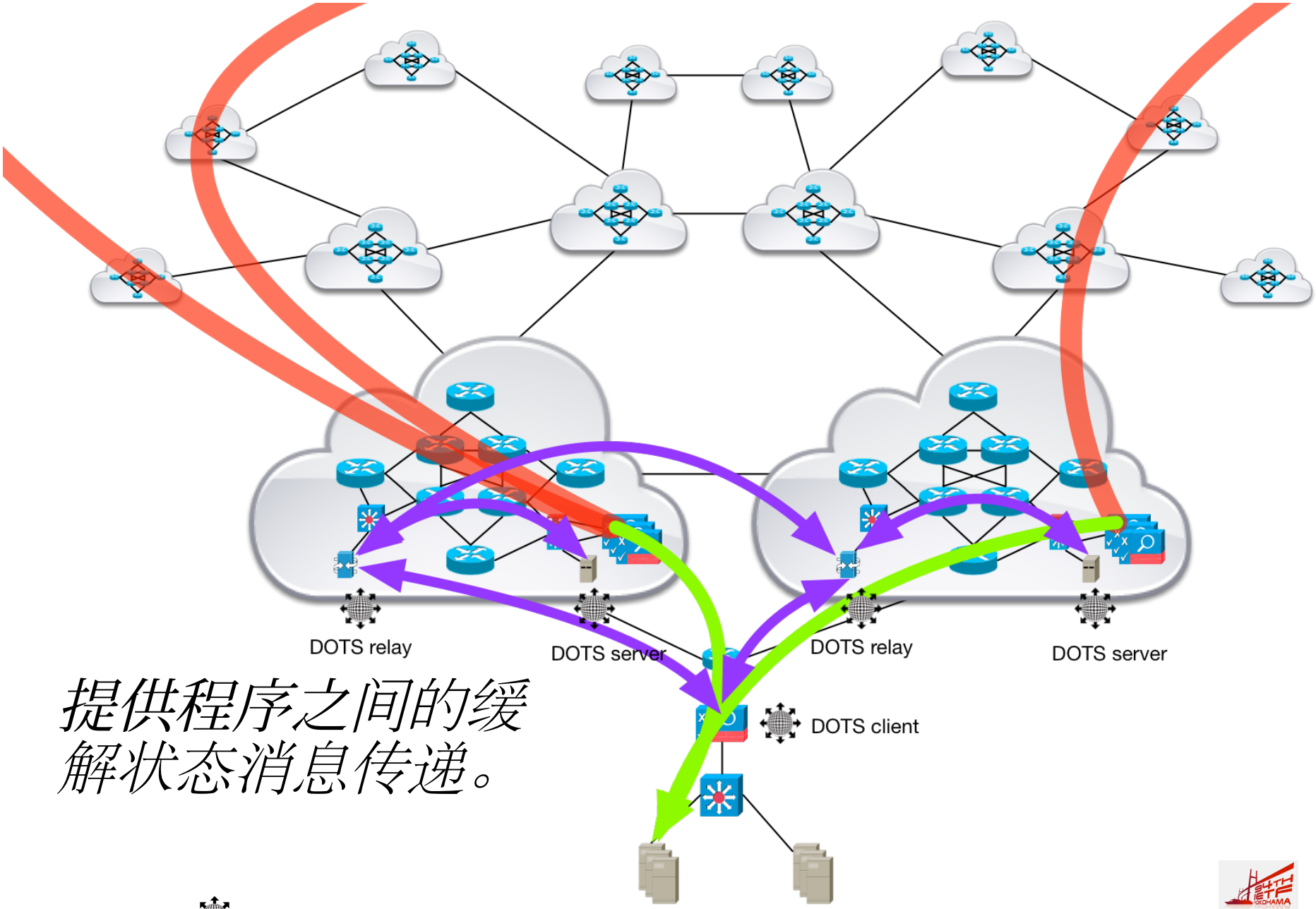


4.1.1 – 多个上游分布式拒绝服务缓解提供商的网络变化


DOTS relay
DOTS server
DOTS relay
DOTS server
DOTS client

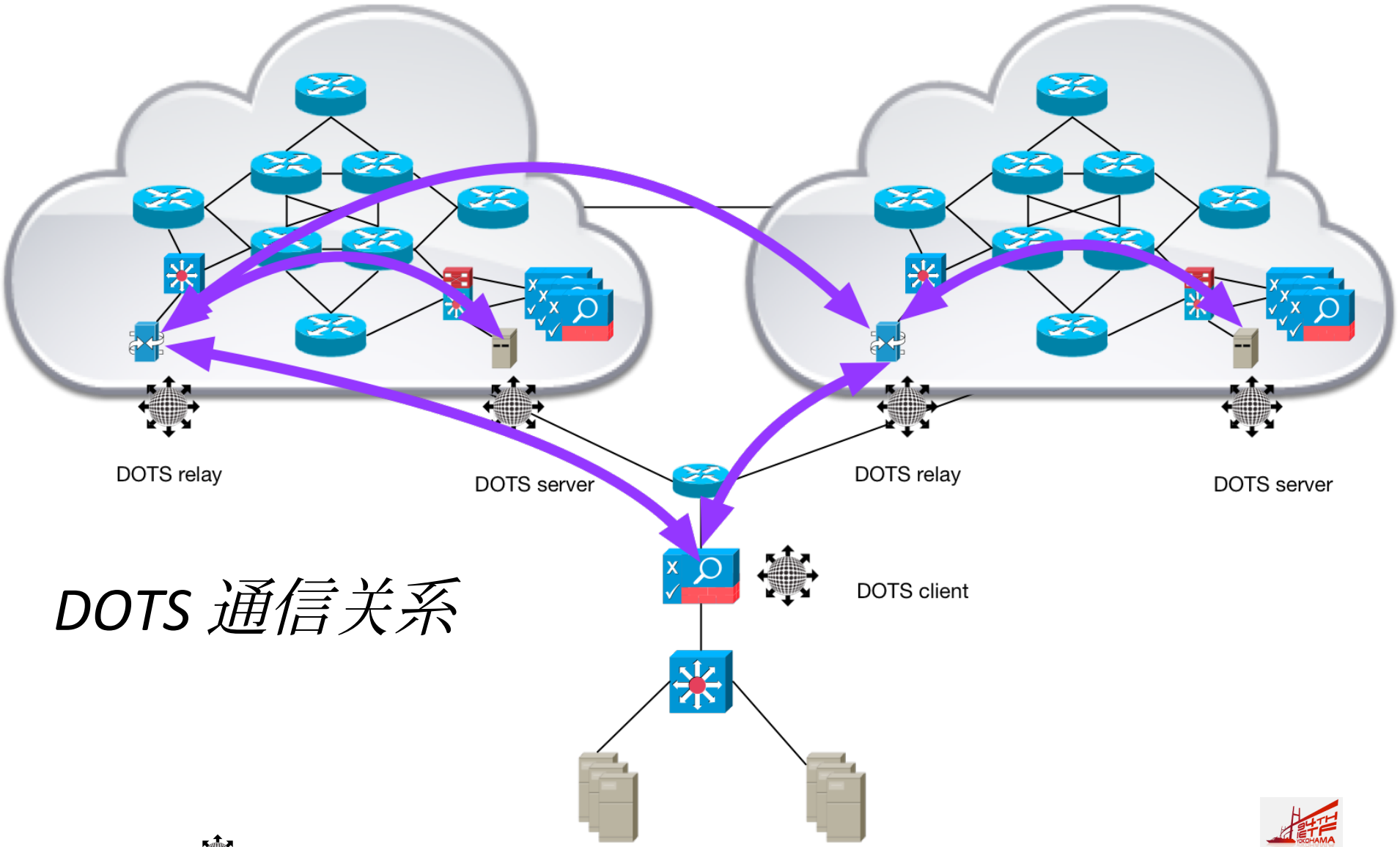


缓解措施正在进行中。



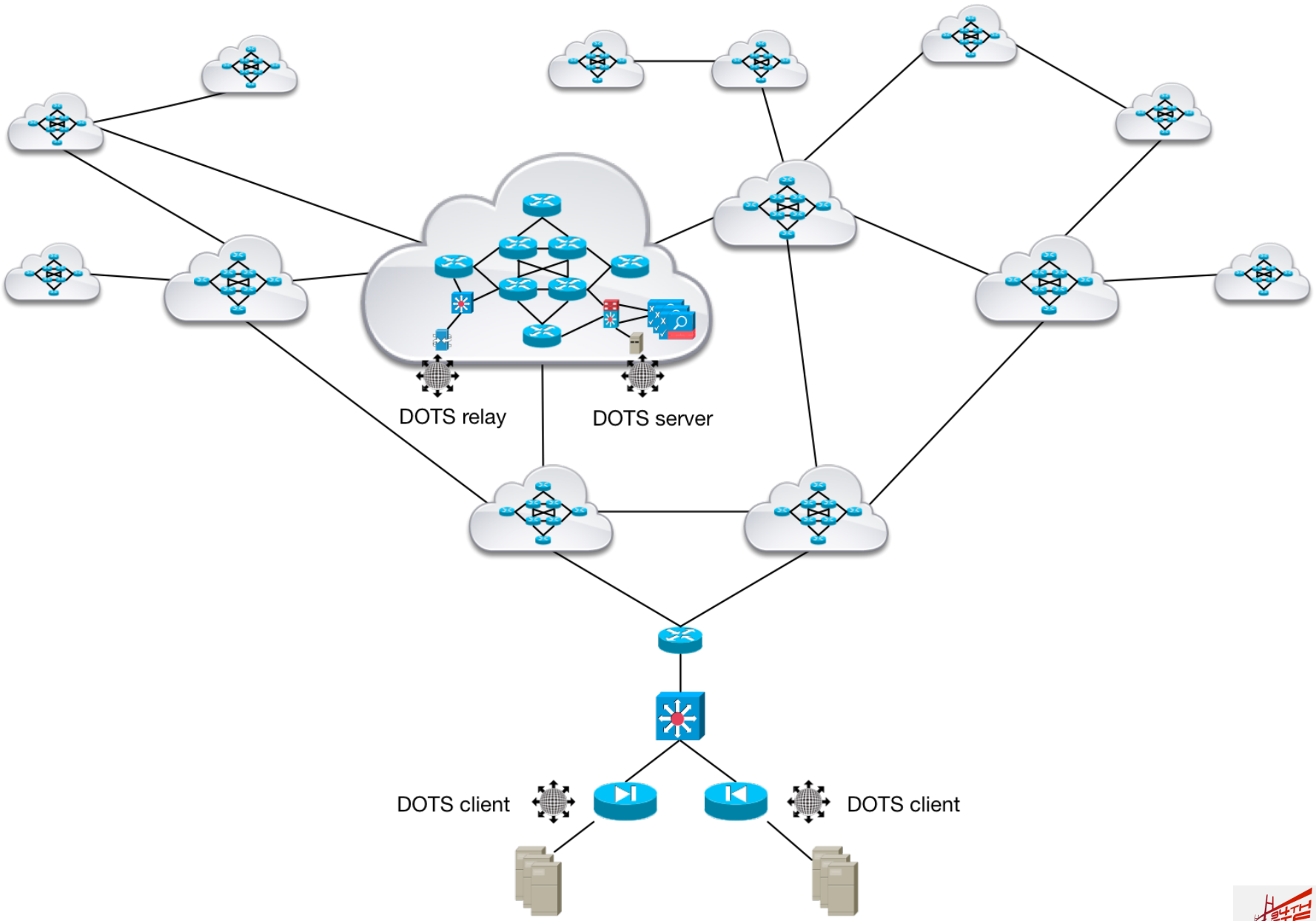
提供程序之间的缓解状态消息传递。

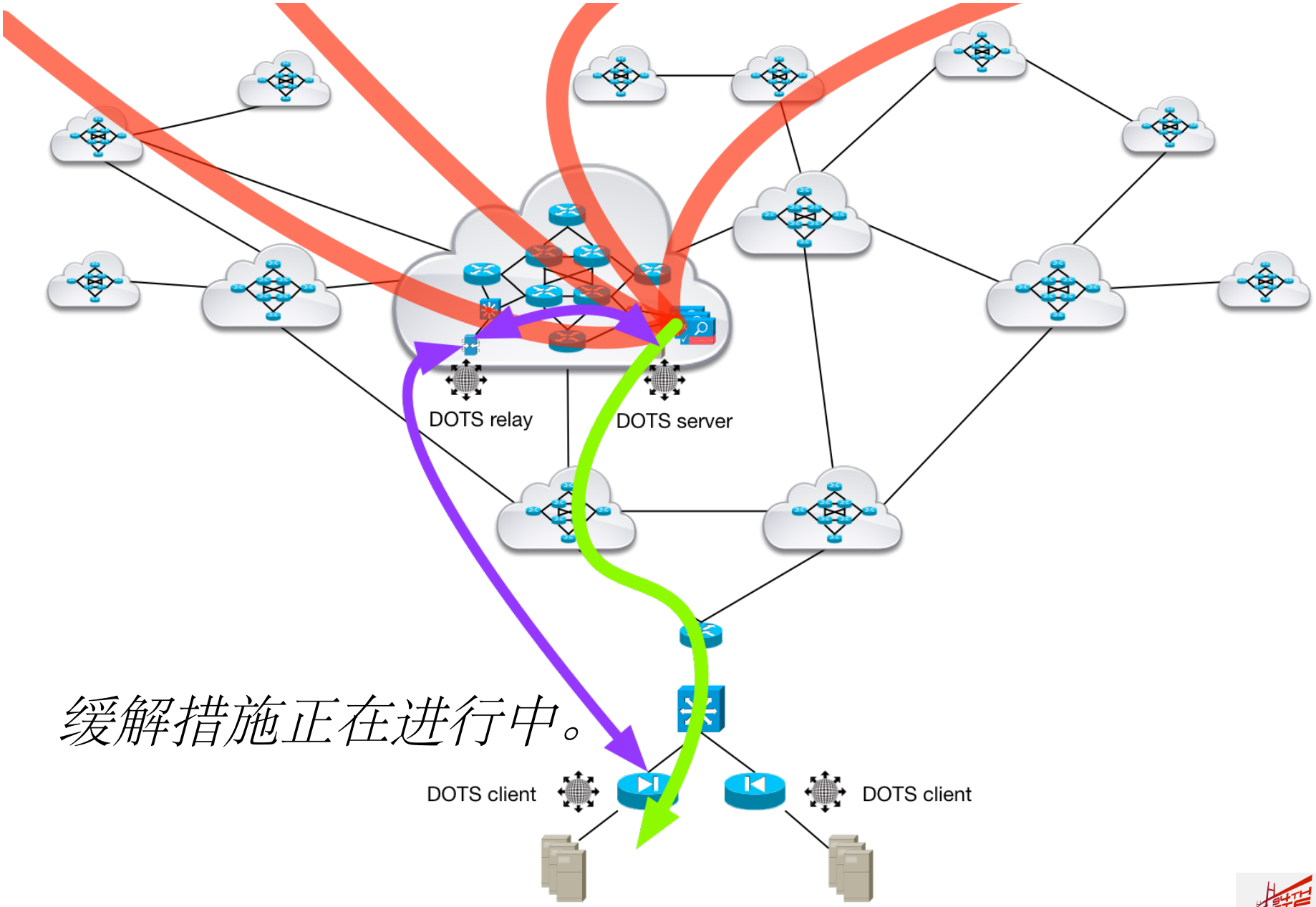
DOTS 通信关系



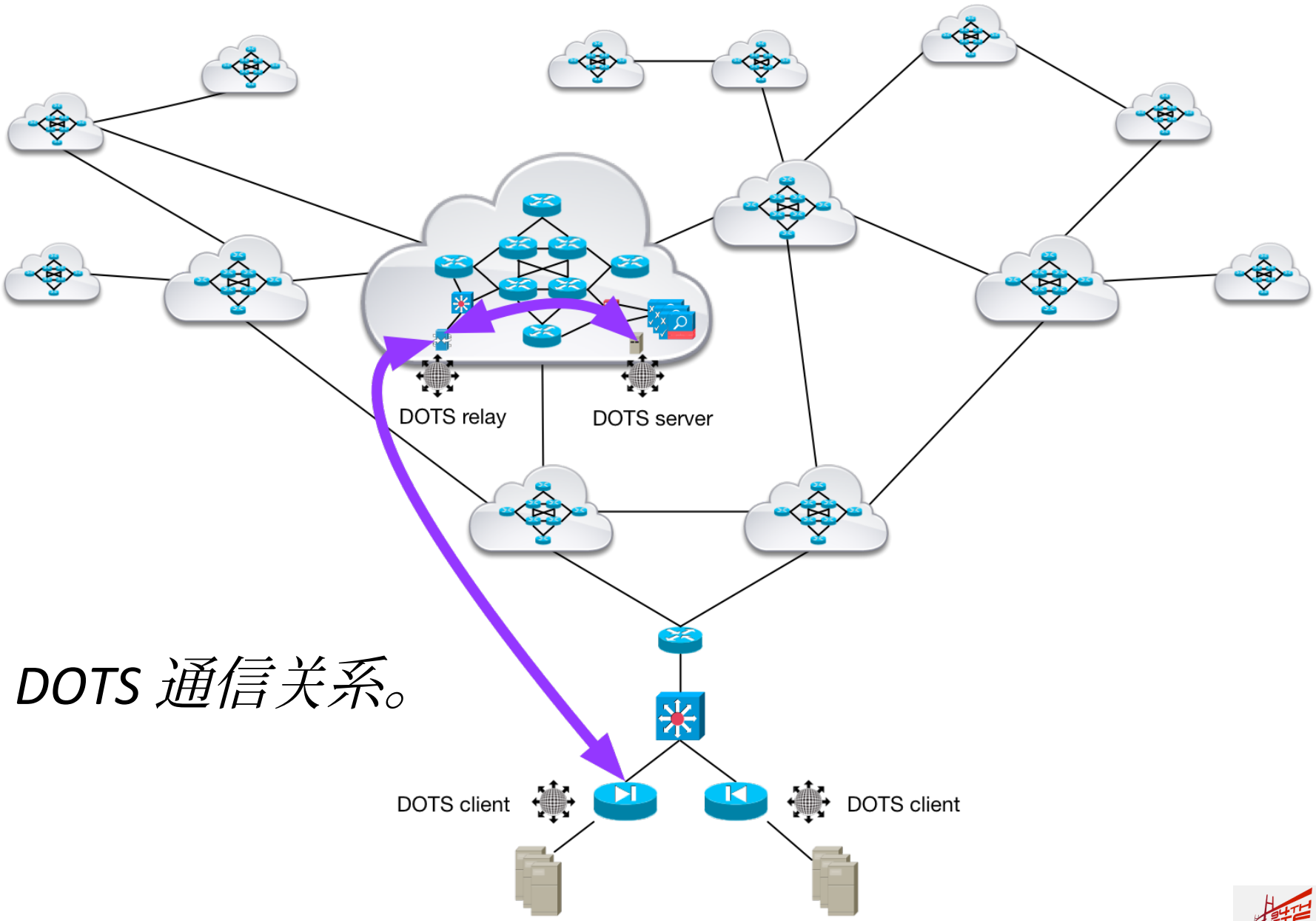
DOTS WG

4.1.2 - 网络基础设施设备请求上游分布式拒绝服务缓解


DOTS relay
DOTS server
DOTS client
DOTS client

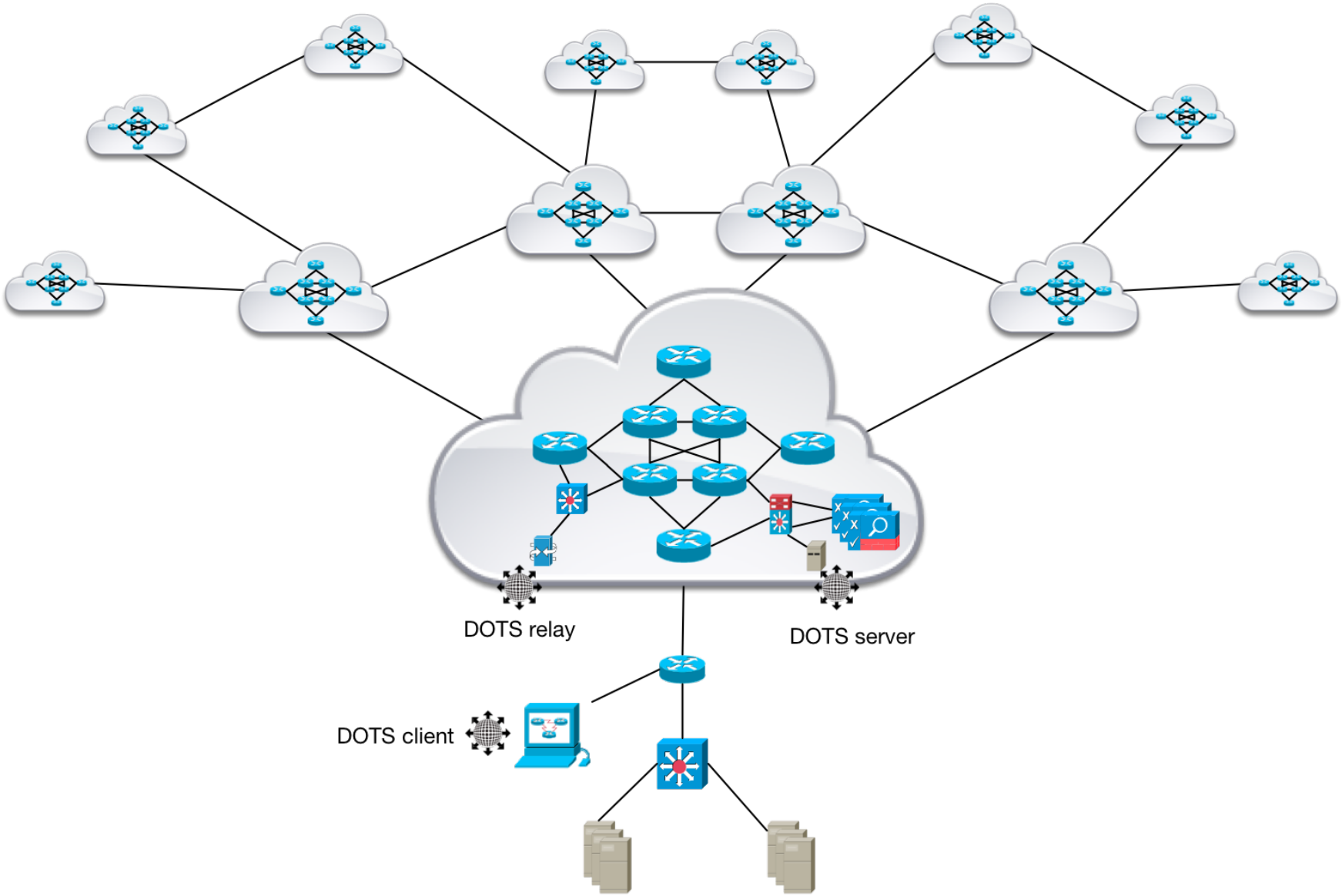


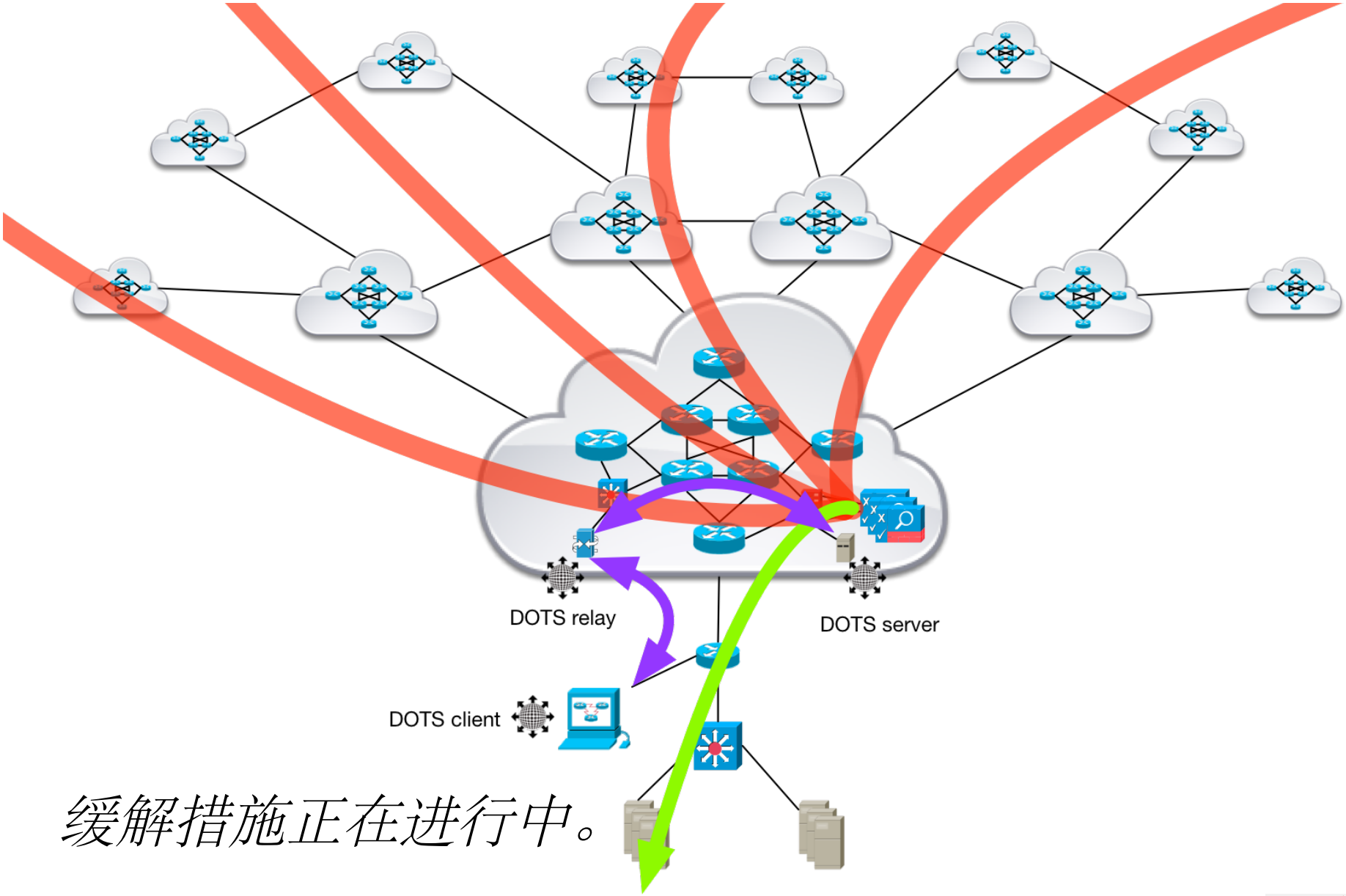
缓解措施正在进行中。



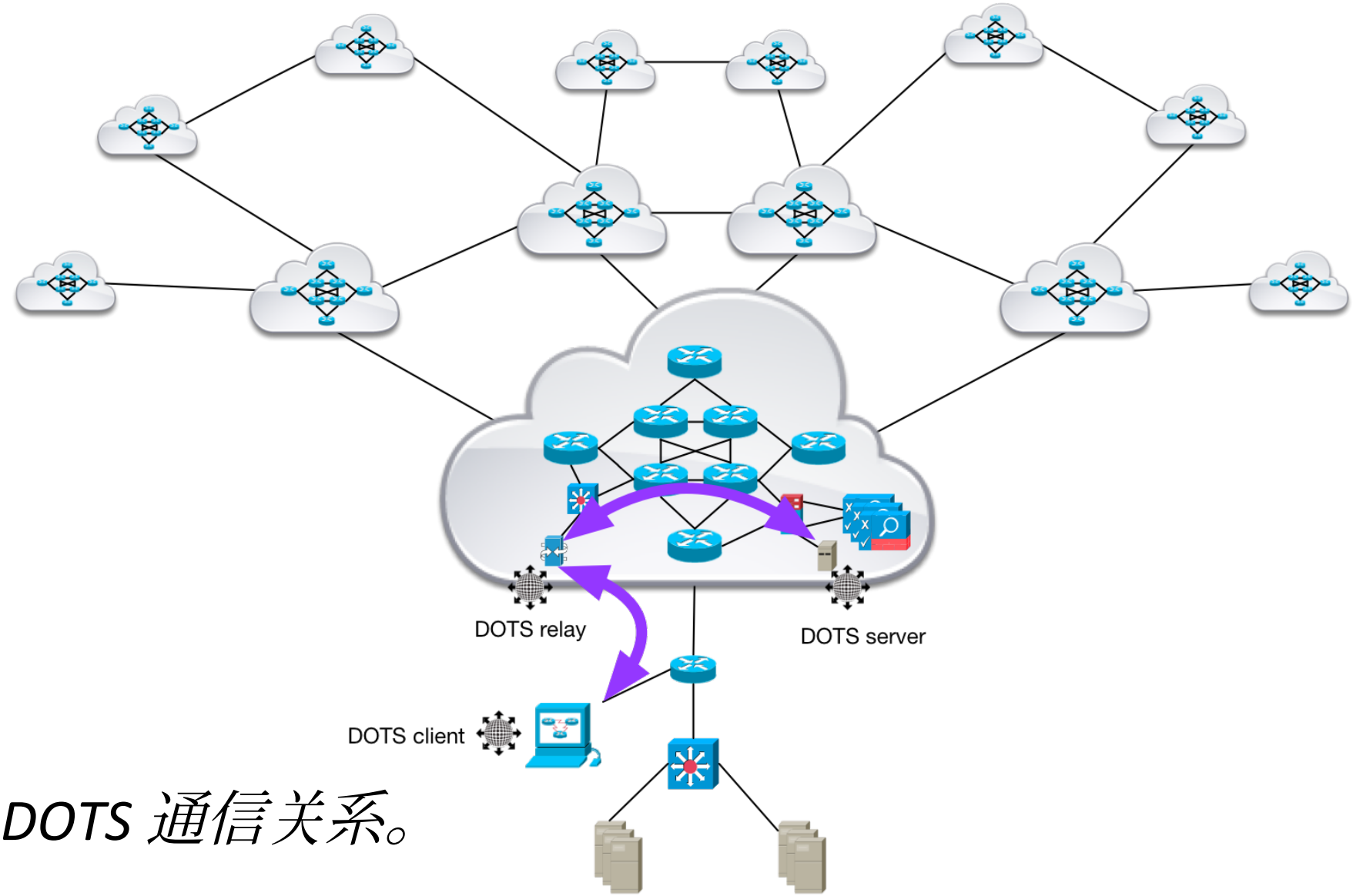
DOTS 通信关系。

4.1.3 -攻击遥测检测/分类系统请求上游分布式拒绝服务缓解


DOTS relay
DOTS server
DOTS client

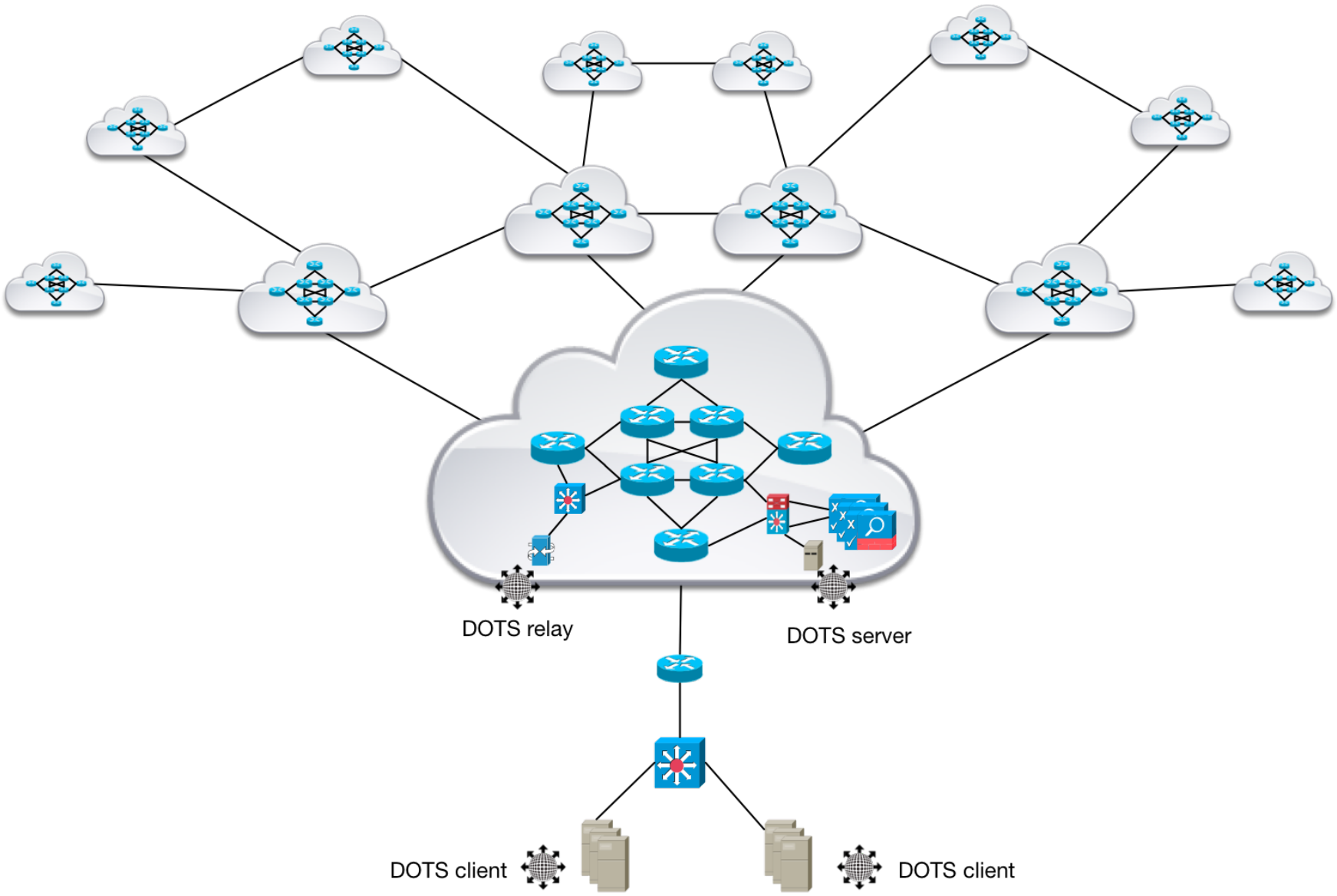


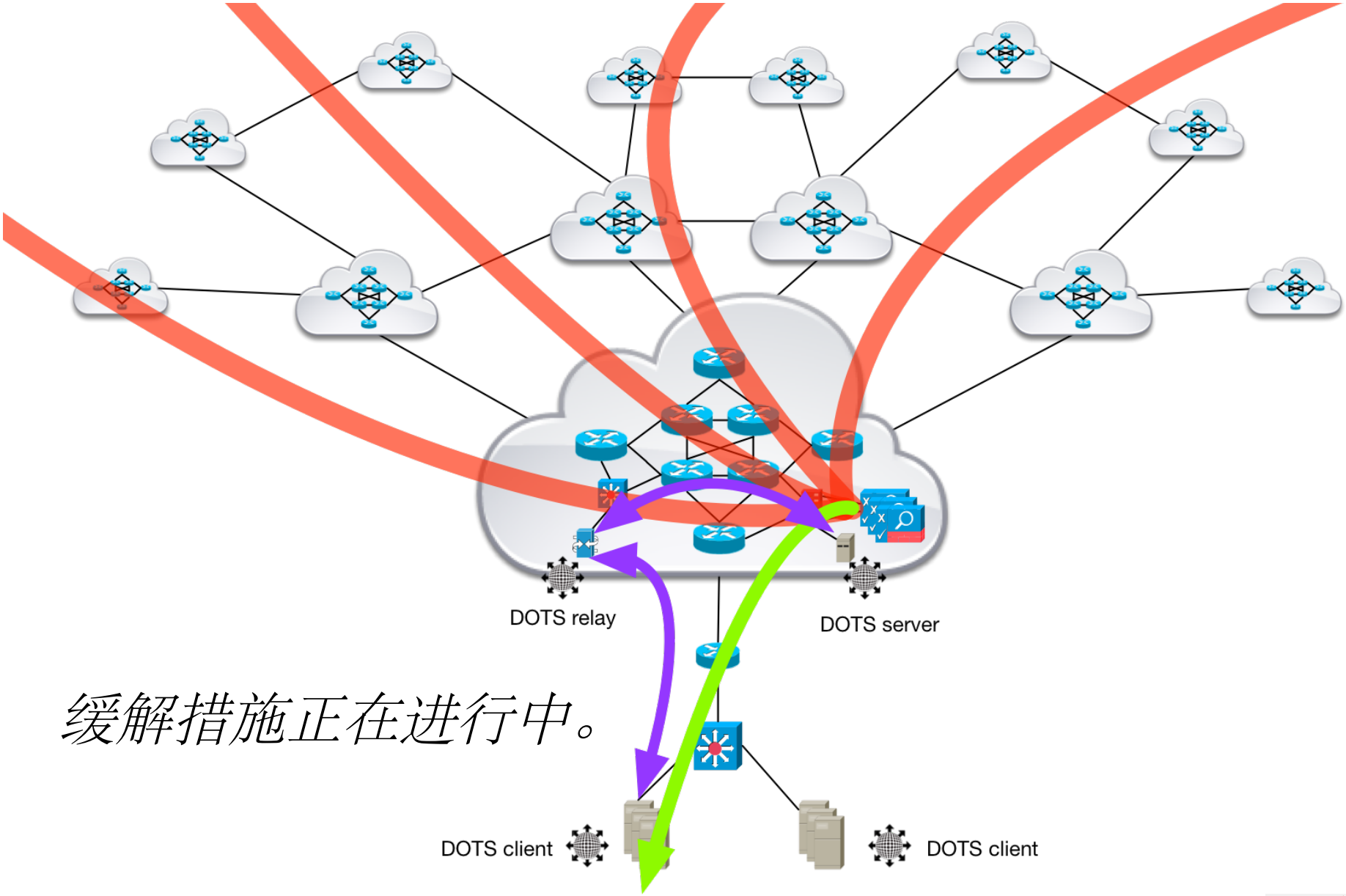
缓解措施正在进行中。



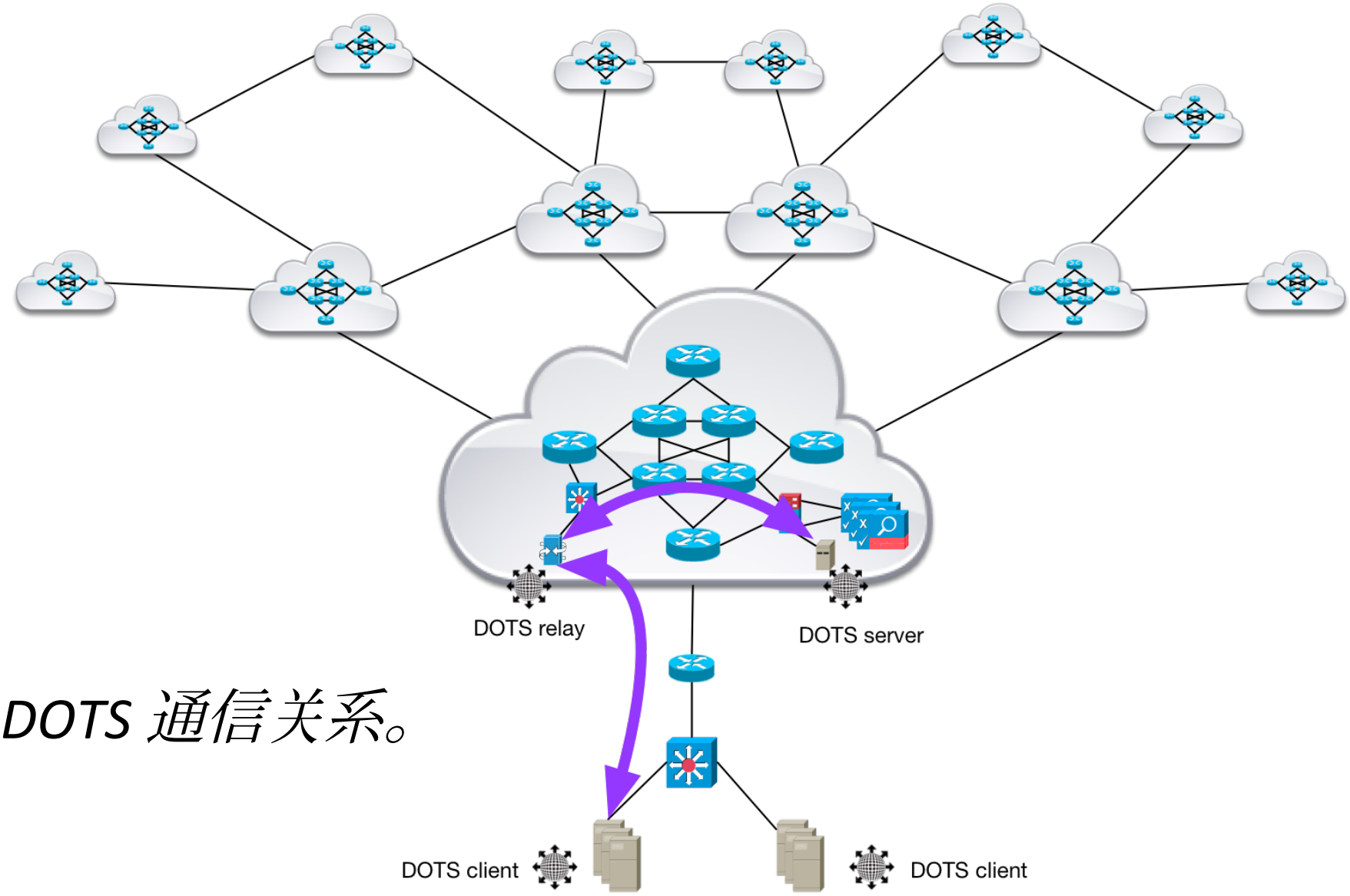
DOTS 通信关系。

4.1.4 -目标服务/应用程序请求上游分布式拒绝服务缓解


DOTS relay
DOTS server
DOTS client
DOTS client

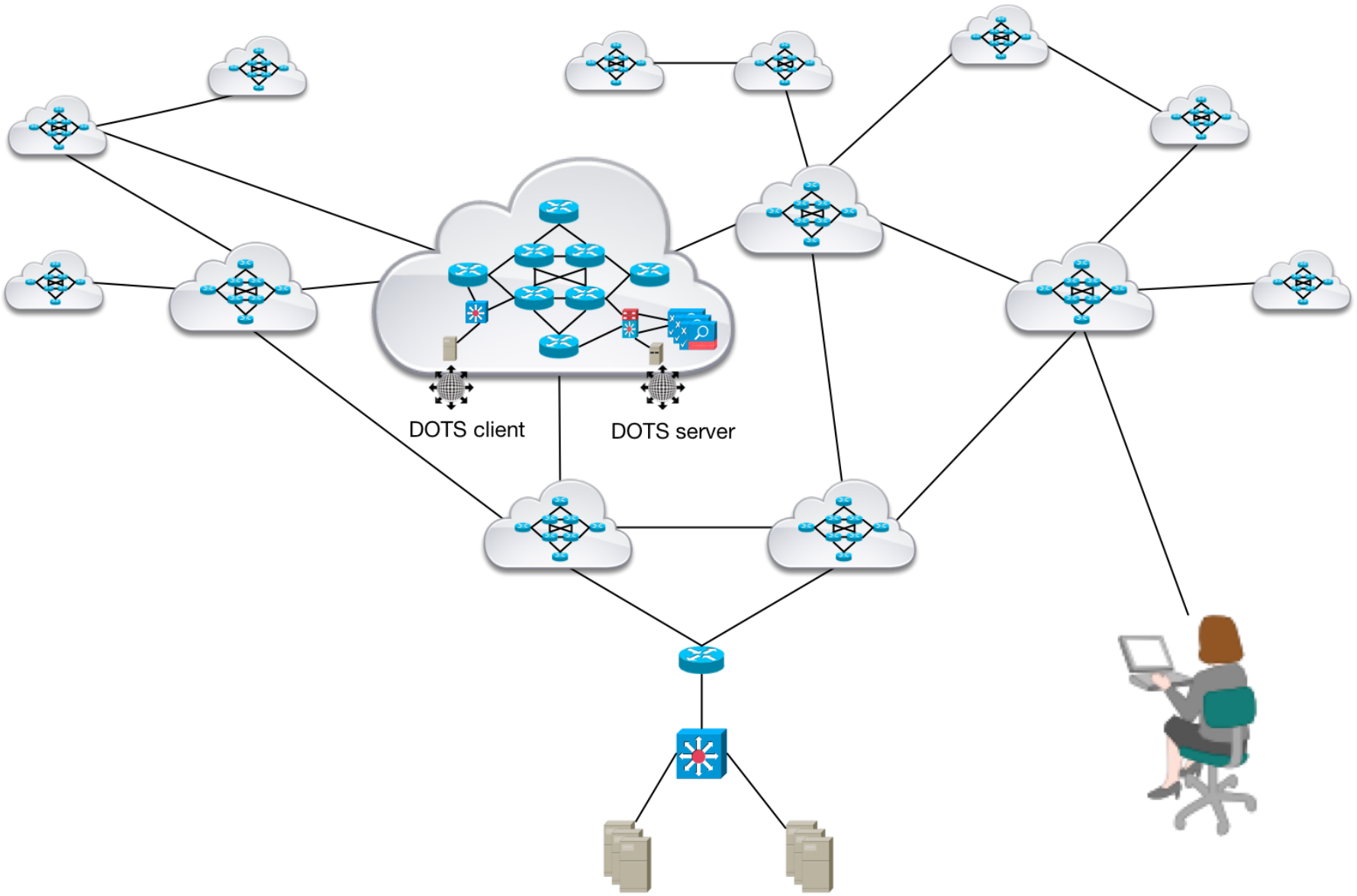


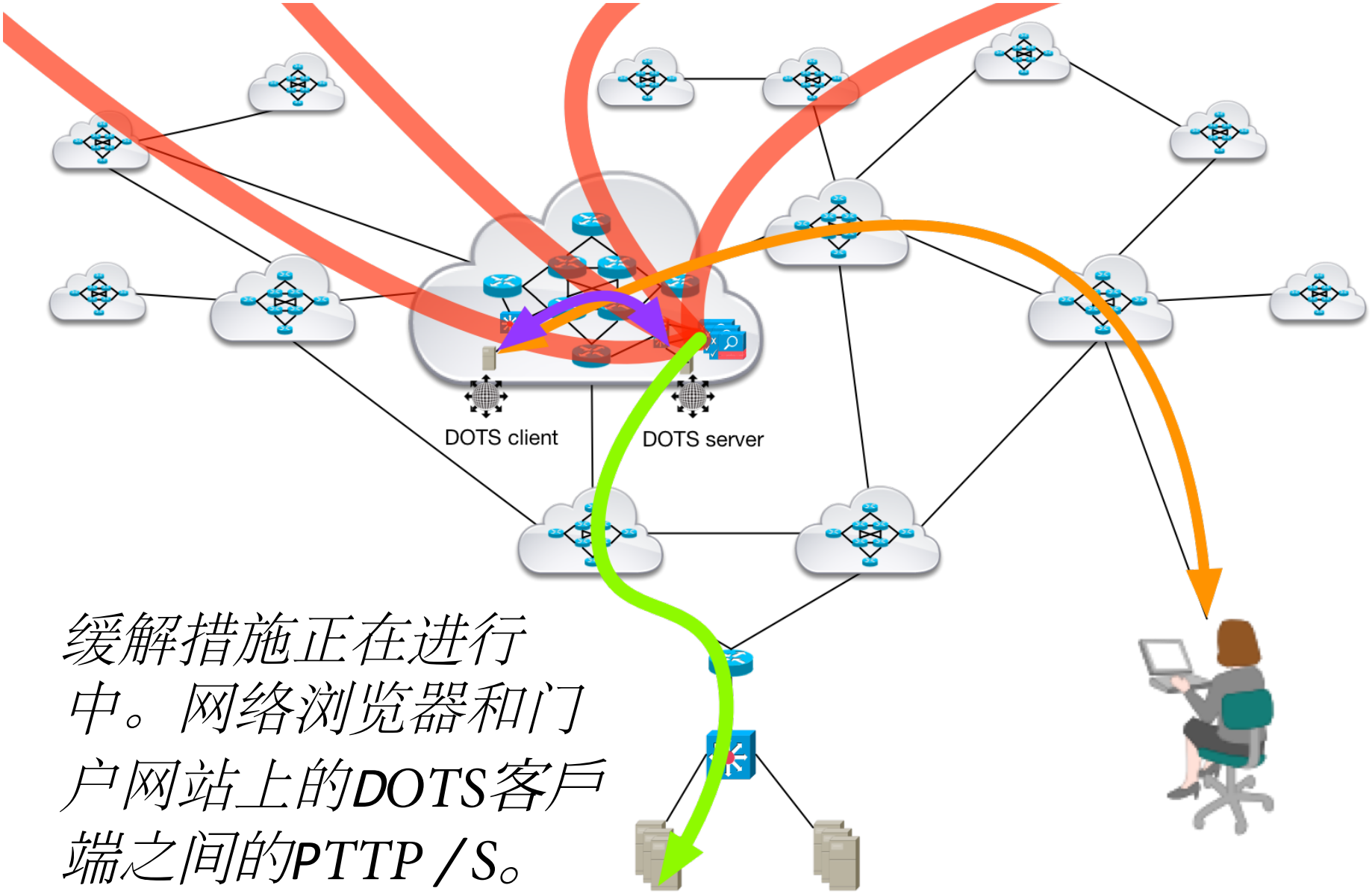
缓解措施正在进行中。



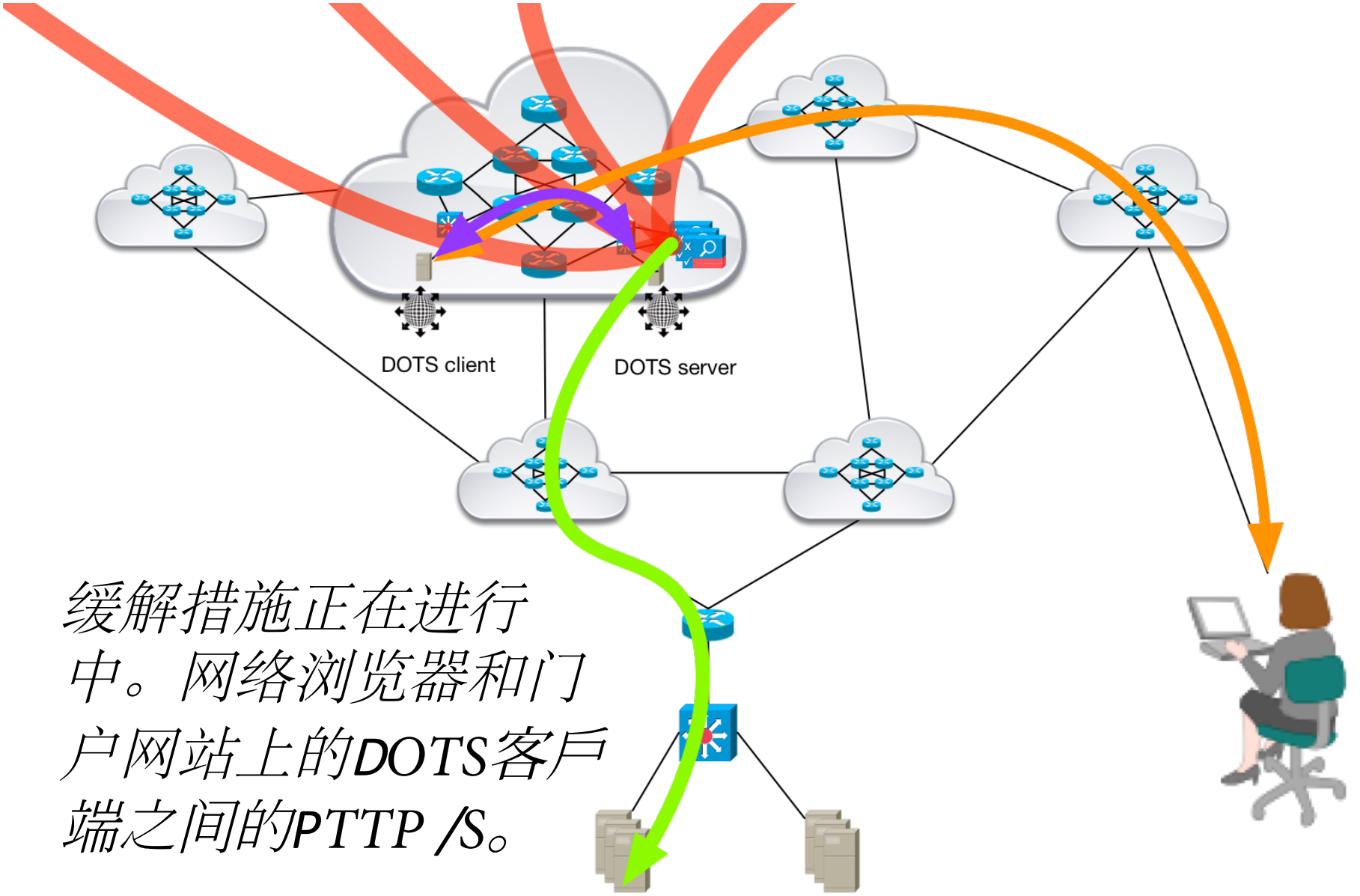
DOTS 通信关系。

4.1.5 -手动向上游缓解器发出门户网站请求


DOTS client
DOTS server

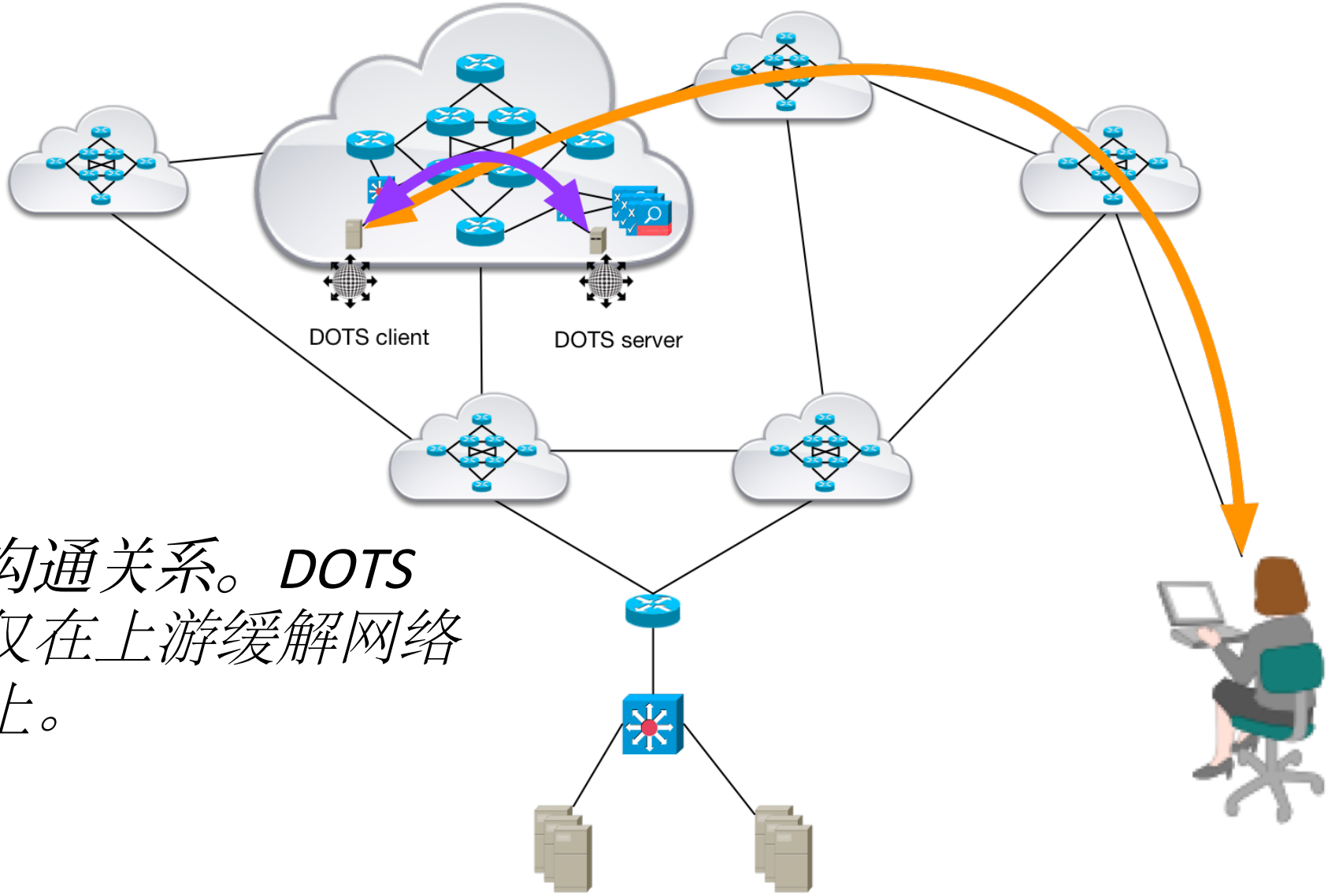


缓解措施正在进行中。网络浏览器和门户网站上的DOTS客戶端之间的PTTP/S。

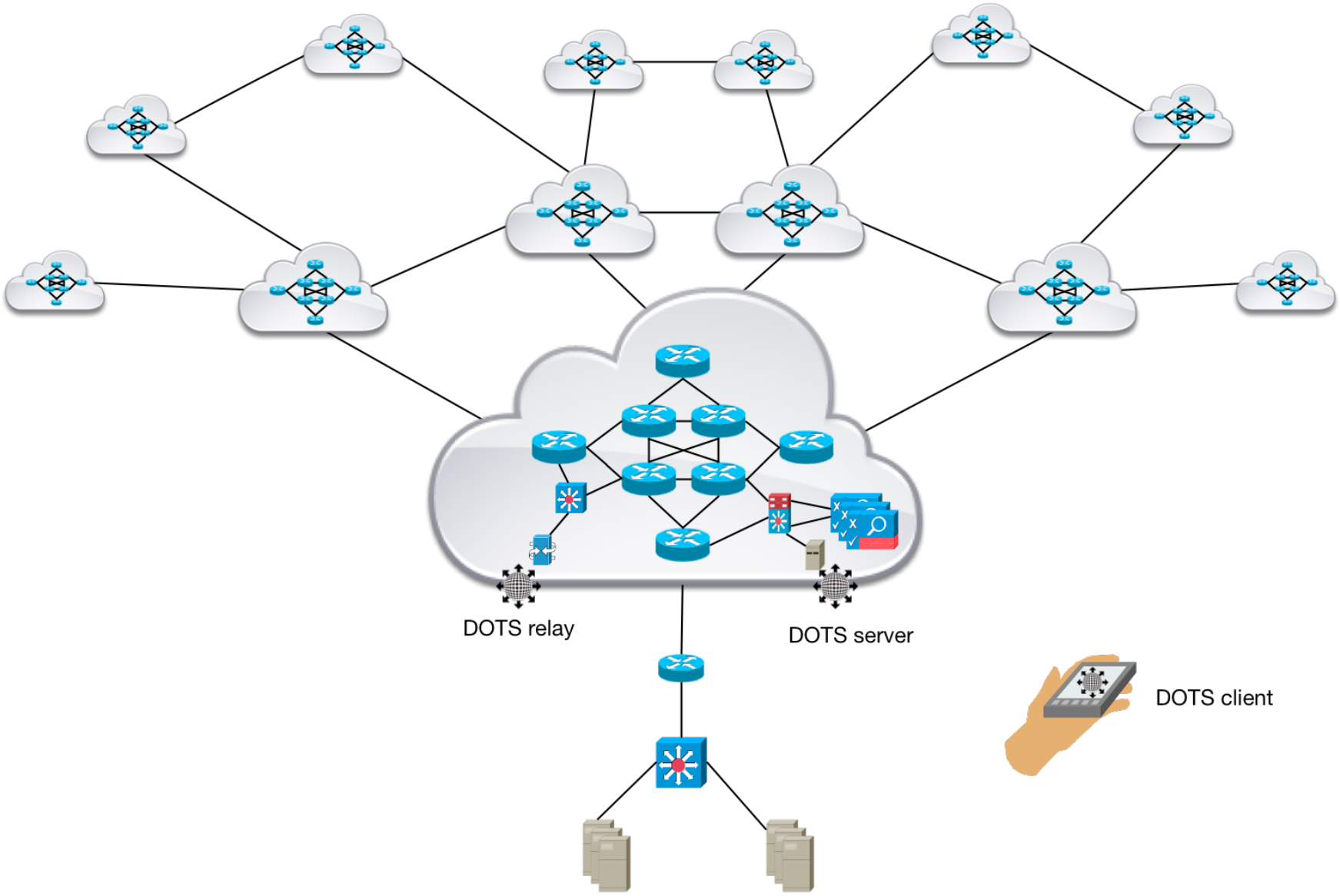


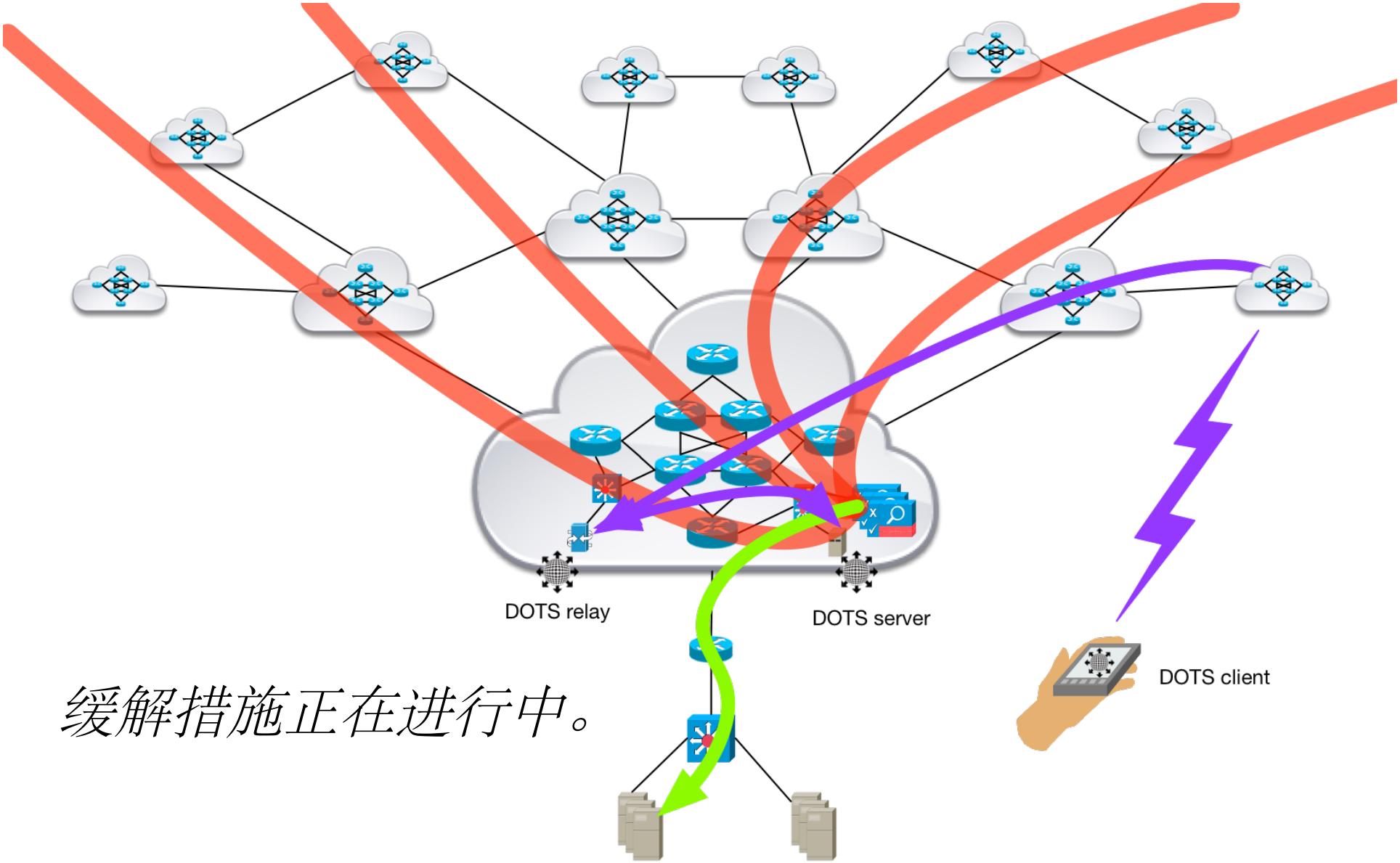
缓解措施正在进行中。网络浏览器和门户网站上的DOTS客戶端之间的PTTP /S。

沟通关系。DOTS仅在上游缓解网络上。

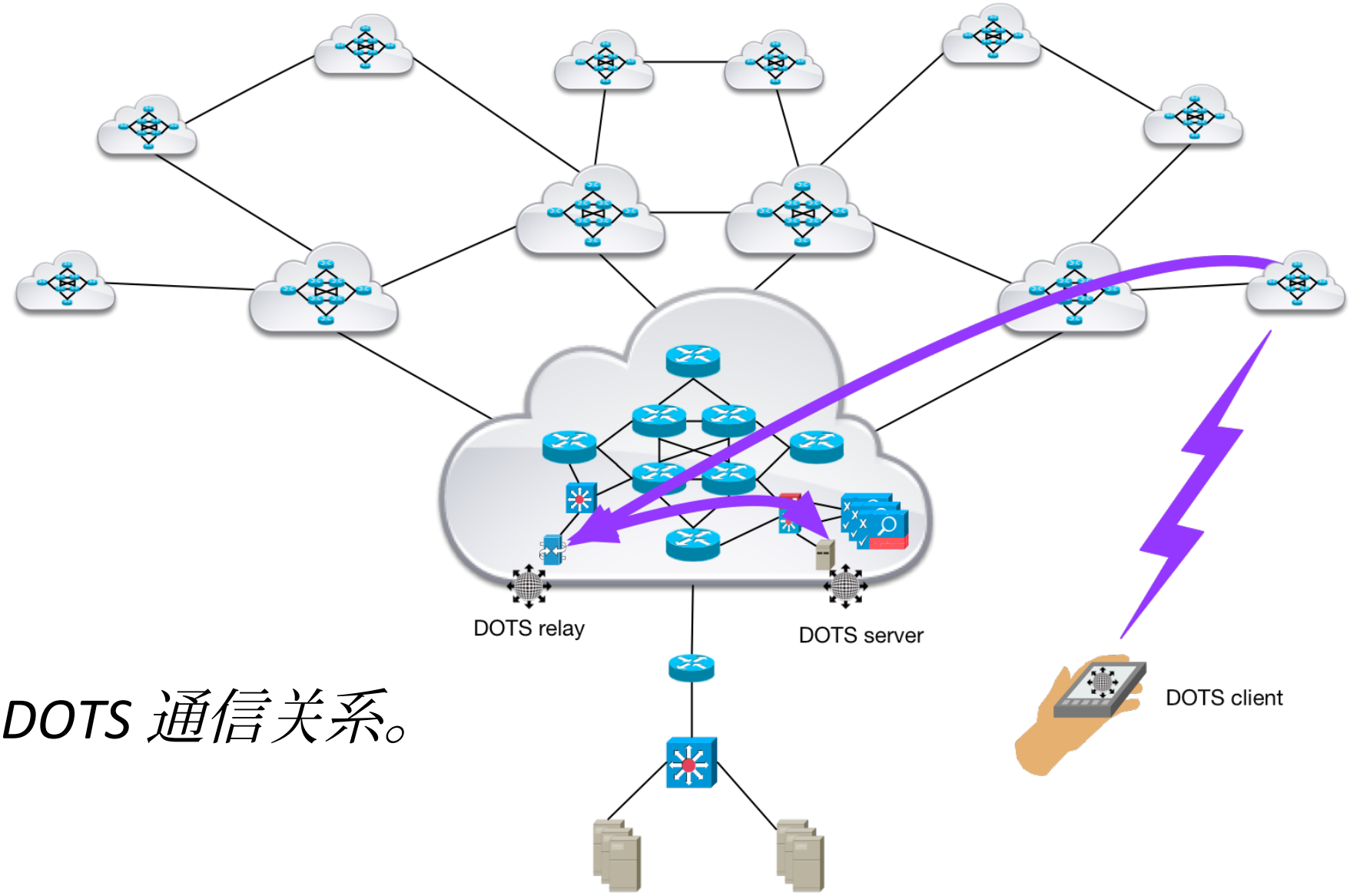


4.1.6 -手动向上游缓解器请求移动设备应用程序


DOTS relay
DOTS server
DOTS client

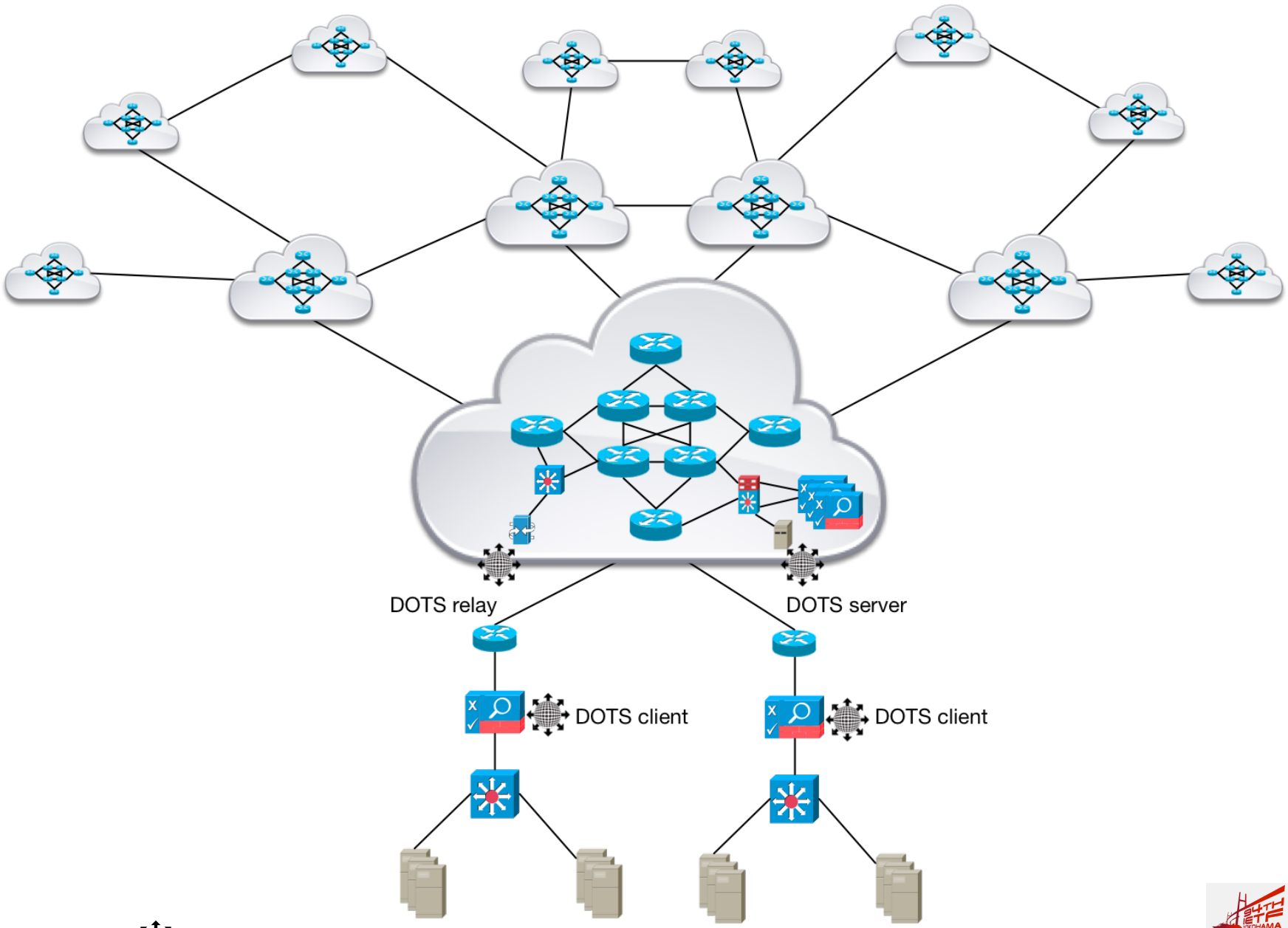


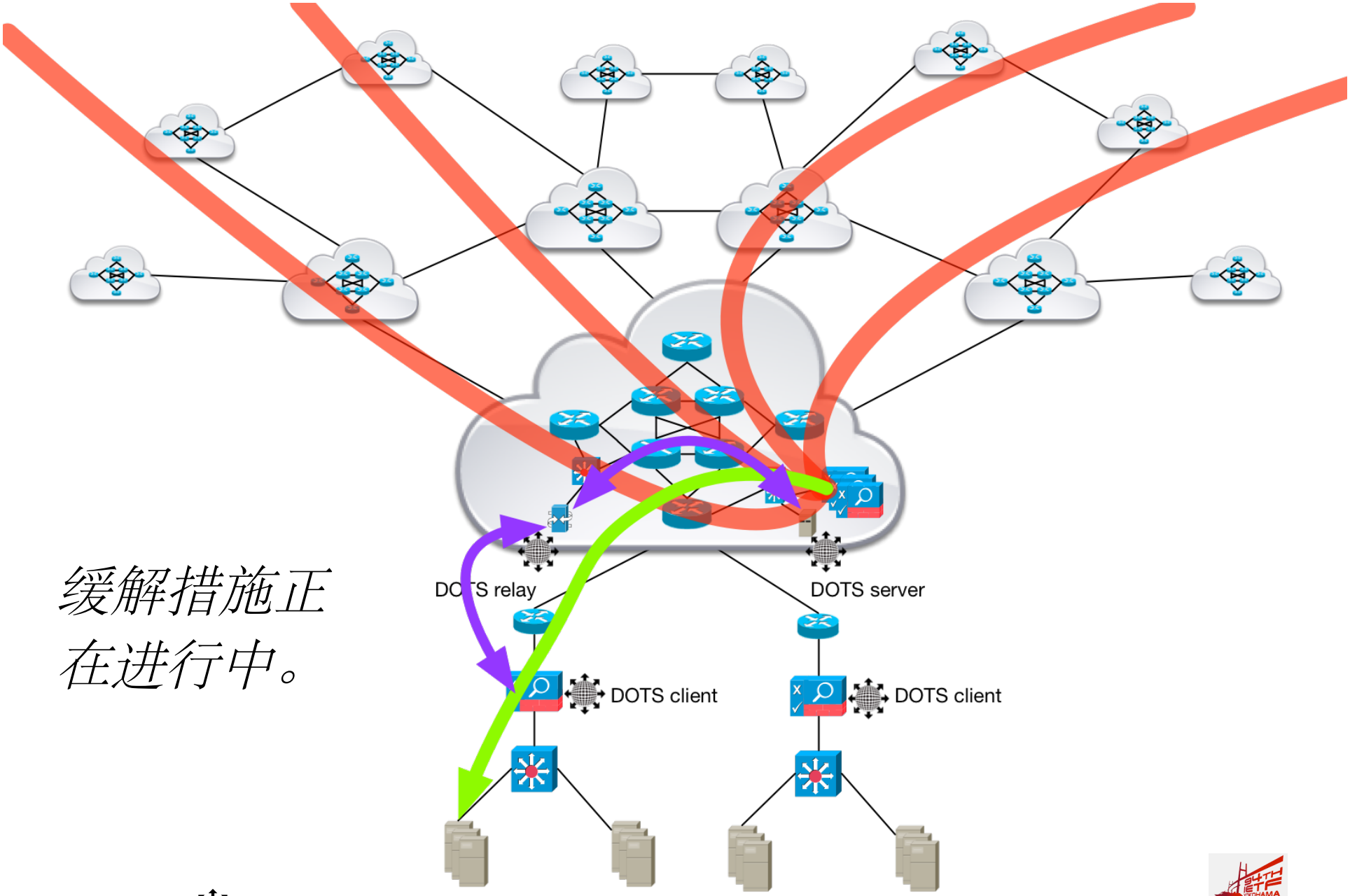
缓解措施正在进行中。



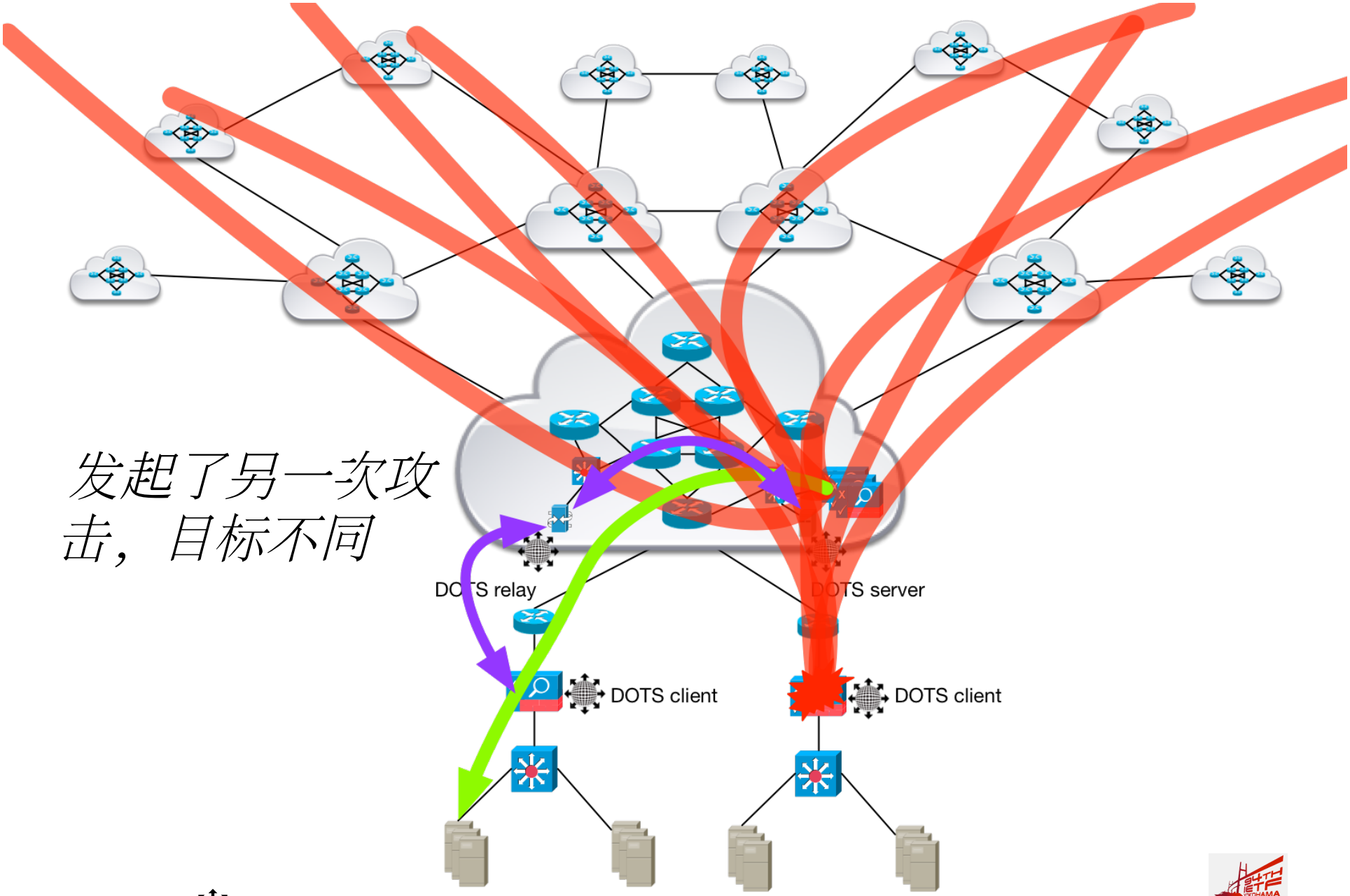
DOTS 通信关系。

4.1.7 -CPE 或PE缓解器未成功请求上游分布式拒绝服务缓解

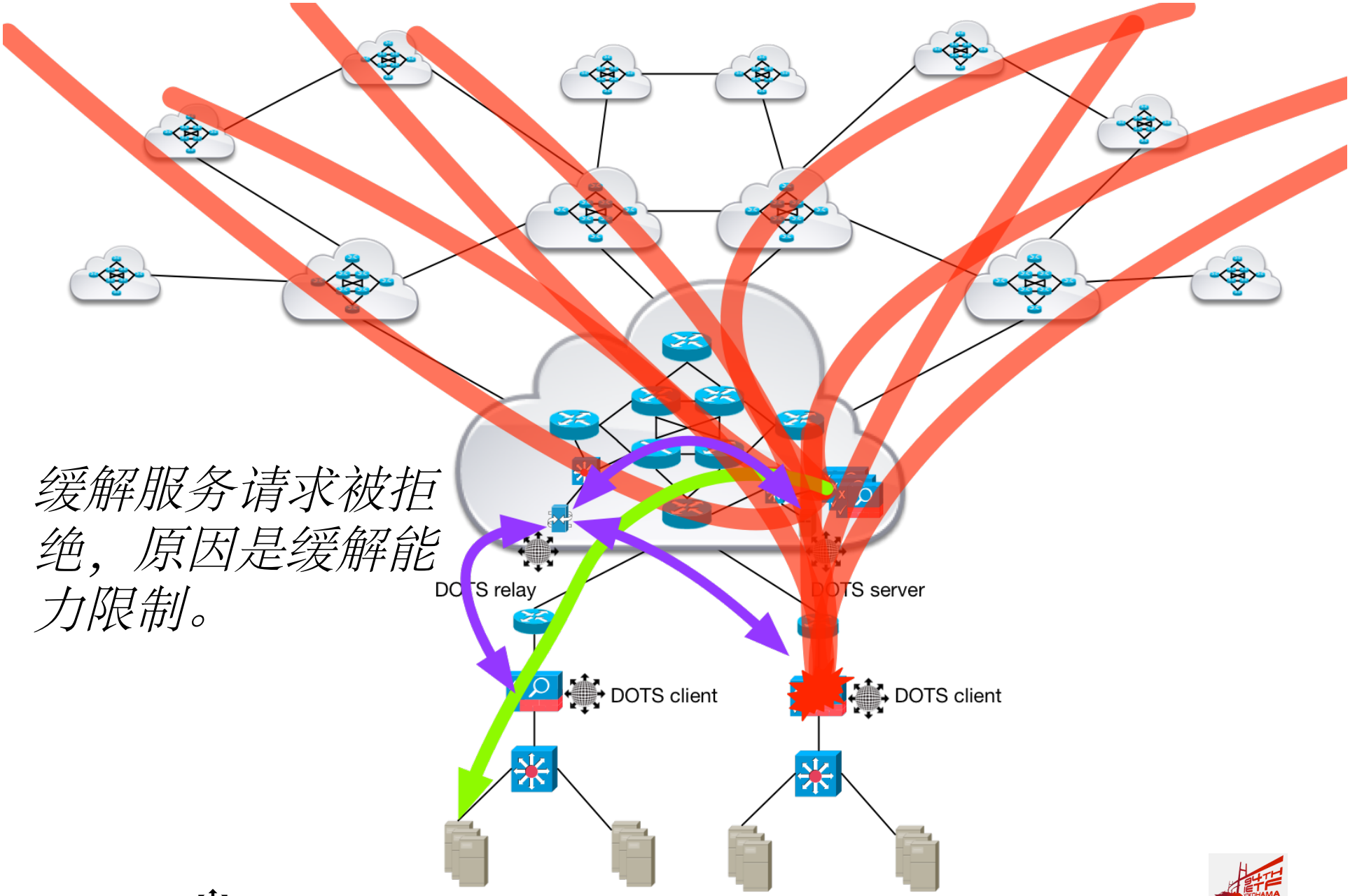

DOTS relay
DOTS server
DOTS client
DOTS client

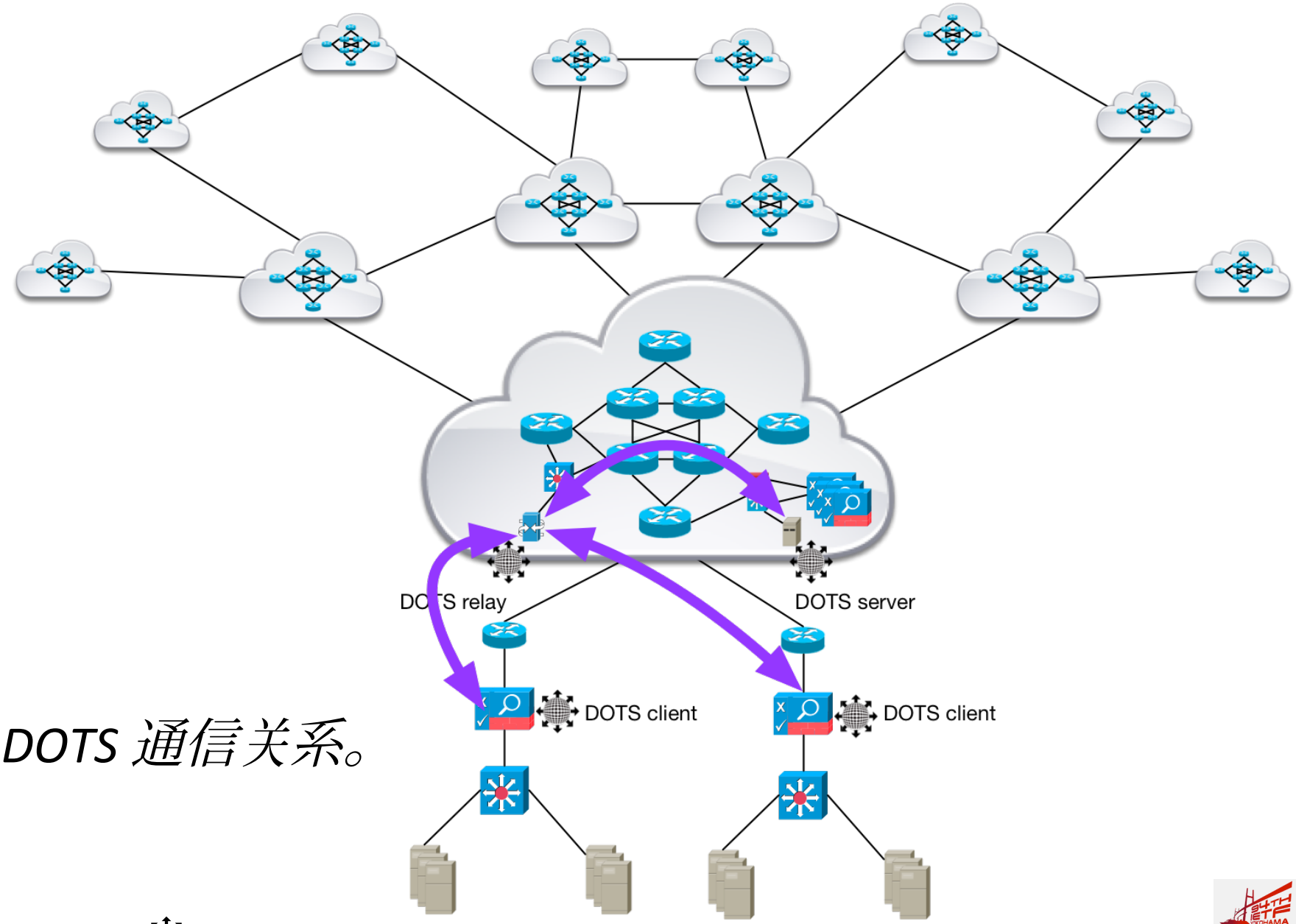


缓解措施正在进行中。


发起了另一次攻击，目标不同
DOTS relay
DOTS server
DOTS client
DOTS client

缓解服务请求被拒绝，原因是缓解能力限制。





DOTS 通信关系。

4.2-辅助用例

4.2.1 –自动注册

- 除了攻击缓解请求，响应和状态消息之外，DOTS对管理任务也很有用。
- 管理任务是有效缓解分布式拒绝服务的重要障碍。
- 具有适当凭据的DOTS客户端可以向上游缓解网络上的DOTS服务器自动注册。
- 这有助于分布式拒绝服务缓解服务的启动，移动/添加 /更改。

4.2.2 –自动供应分布式拒绝服务对策

- 如今，分布式拒绝服务对策供应主要是手动过程，错误和低效可能会成问题。
- 这可能会导致分布式拒绝服务缓解服务配置不足，通常无法针对分布式拒绝服务保护下的资产进行优化。缓解速度快，疗效不佳。
- 在攻击（非常常见的情况）下，入职组织可能会非常具有挑战性。
- 可以利用DOTS注册和缓解状态请求的“自描述”性质来自动执行对策选择，设置和调整过程。
- 攻击期间从DOTS客户端到DOTS服务器的缓解功效反馈可用于实时缓解调整和优化。

4.2.3 –信息性分布式拒绝服务攻击通知第三方

- 除了受攻击的组织向上游缓解器发出的服务请求之外，DOTS还可以用于向感兴趣的和授权的第三方发送分布式拒绝服务攻击通知和状态消息。
- 在某些情况下，自动提供经济或第三级“备份”缓解提供商，安全研究人员，供应商，执法机构，监管机构等的攻击通知和状态消息可能会有所帮助。
- 与第三方的任何此类信息共享应仅根据所有相关法律，法规，合同义务，隐私和保密协议进行。

后续使用步骤

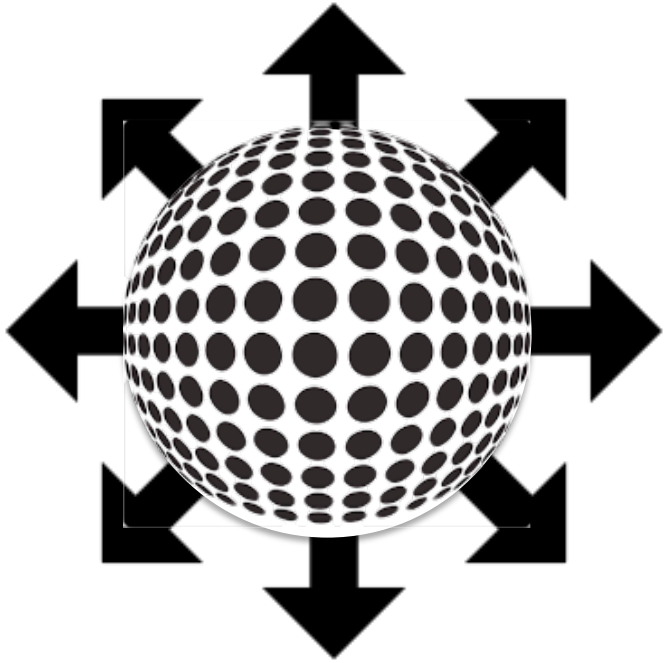
的待办事项清单 draft-dots-ietf-use-cases-01

- 修正错别字（哦！）。
- 删除重复的摩擦。
- Wordsmith措辞清晰。
- 通过“差异”展示用例-即，指与其他用例的共性，强调每个用例所特有的特定因素。
- 使术语定义与dots-ietf-需求草案保持一致。
- 添加用例，说明在原始网络上抑制分布式拒绝服务攻击流量并在中间网络上进行过滤。
- 添加用于说明特定PE-PE方案的用例（例如，要求额外的分布式拒绝服务缓解能力的“溢出”请求等）。

要求工作组参与者提供反馈

- 我们应该添加什么？
- 我们应该删除什么？
- 我们应该改变什么？
- 我们是否应该在每个用例中包含与本演示文稿中的4.1.1相似的变体（通过“差异”）？
- 其他输入？

本演讲 – 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