苏宁易购

全站HTTPS

CONTENT

为什么我们要使用HTTPS？ 01

苏宁易购全站HTTPS方案概述 02

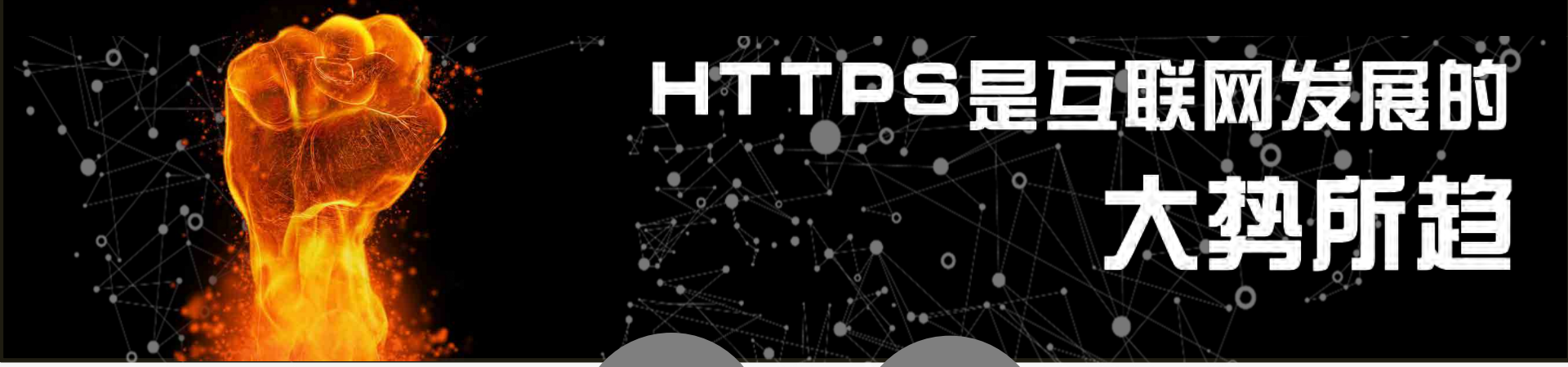
HTTPS系统改造篇 03

HTTPS性能优化篇 04

HTTPS灰度上线篇 05

01

为什么我们要使用HTTPS



篡改 X

监听 X

劫持 X

文明传输

窃取 X

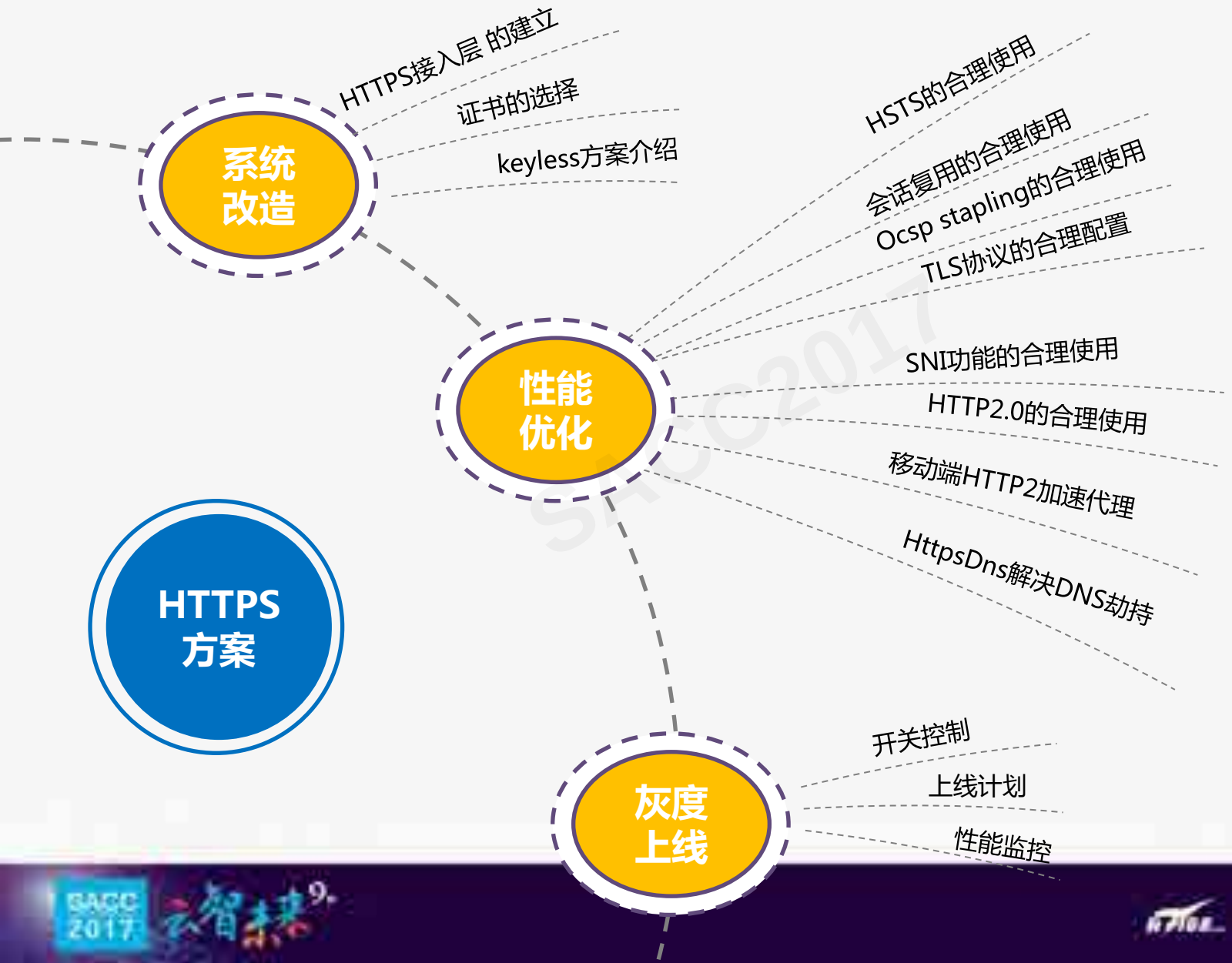
焕新节

全友家居官方旗舰店
绿色设计国际贡献奖
O2O

02

苏宁易购全站HTTPS方案概述

苏宁易购全站HTTPS方案概述



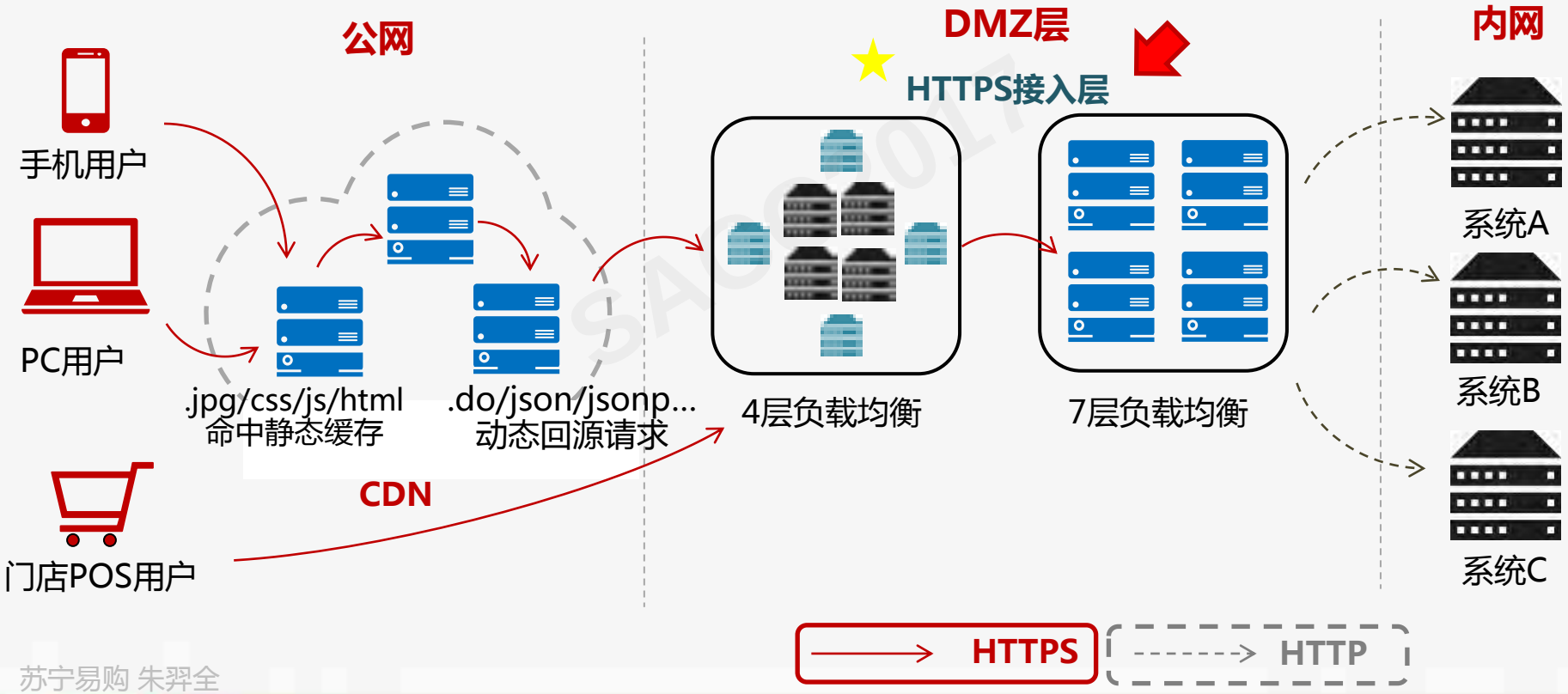
SACC2017

03

HTTPS系统改造篇

HTTPS接入层定义

- 尽早完成SSL握手
- 统一接入与调度，业务系统不需要做调整
- 统一优化与升级，提高接入层性能与安全性



证书选择细节

证书可以分为三类：

DV证书	Domain Validation Certificate
OV证书	Organization Validation Certificate
EV证书	Extended Validation Certificate

根据以下四点选择证书：

1. 证书主机名匹配
2. 是否支持多域名和泛域名
3. 签名算法：散列算法建议使用SHA256
4. 证书链：递归签名，校验合法性，域名证书-中间证书-根证书

SACC2017

证书选择细节

多域名：suning.com、suning.cn、suning.vip

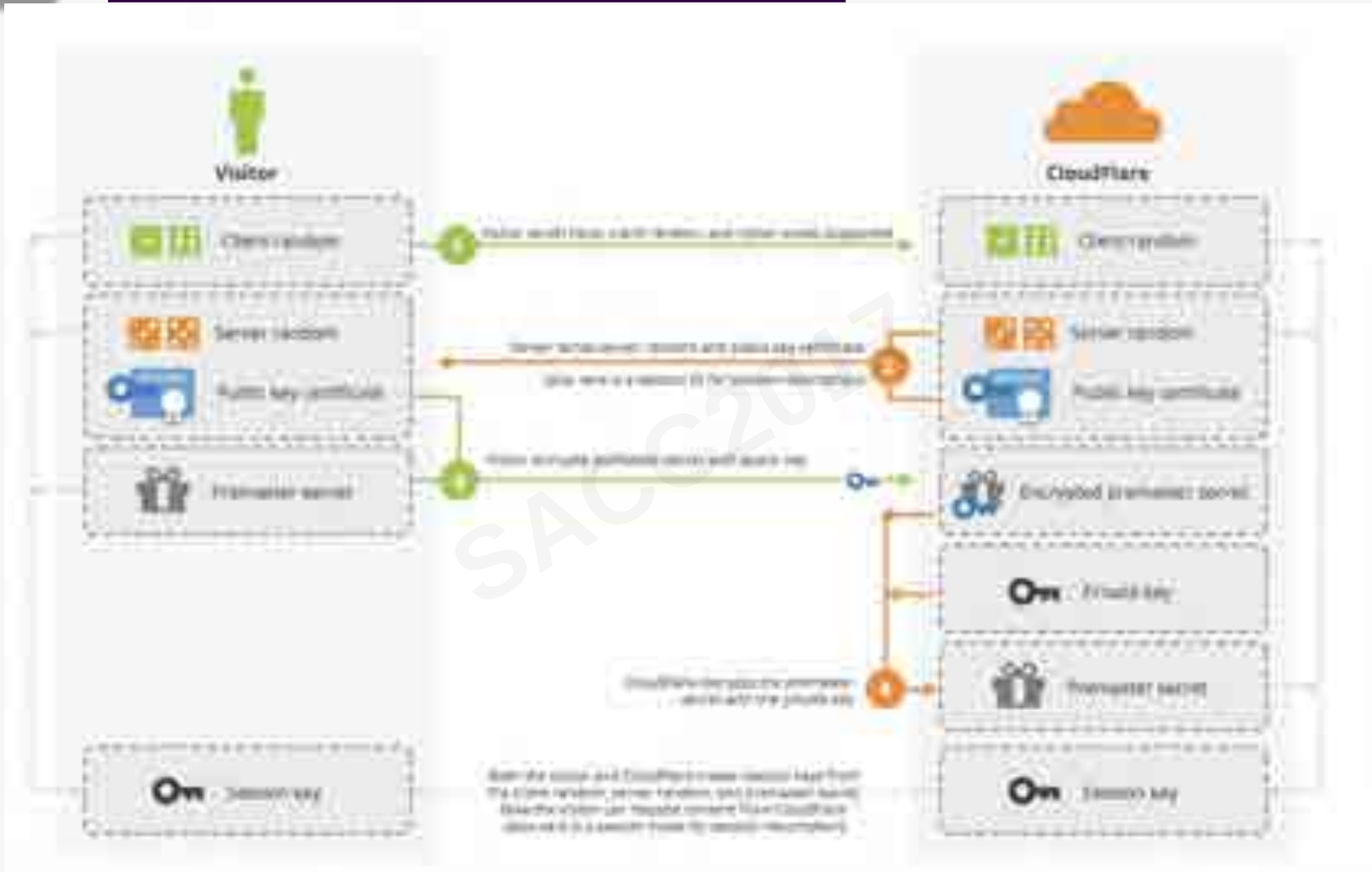
泛域名：*.suning.com的泛域名证书可以匹配www.suning.com、passport.suning.com等。

```
*.tmall.com证书支持的域名:

DNS Name=*.tmall.com
DNS Name=*.1688.com
DNS Name=*.3c.tmall.com
DNS Name=*.alibaba.com
DNS Name=*.aliqin.tmall.com
DNS Name=*.alitrip.com
DNS Name=*.aliyun.com
...
DNS Name=taobao.com
DNS Name=taoptaopiao.com
DNS Name=tmall.hk
DNS Name=ttpod.com
DNS Name=xiami.com
DNS Name=tmall.com
```

SACC2017

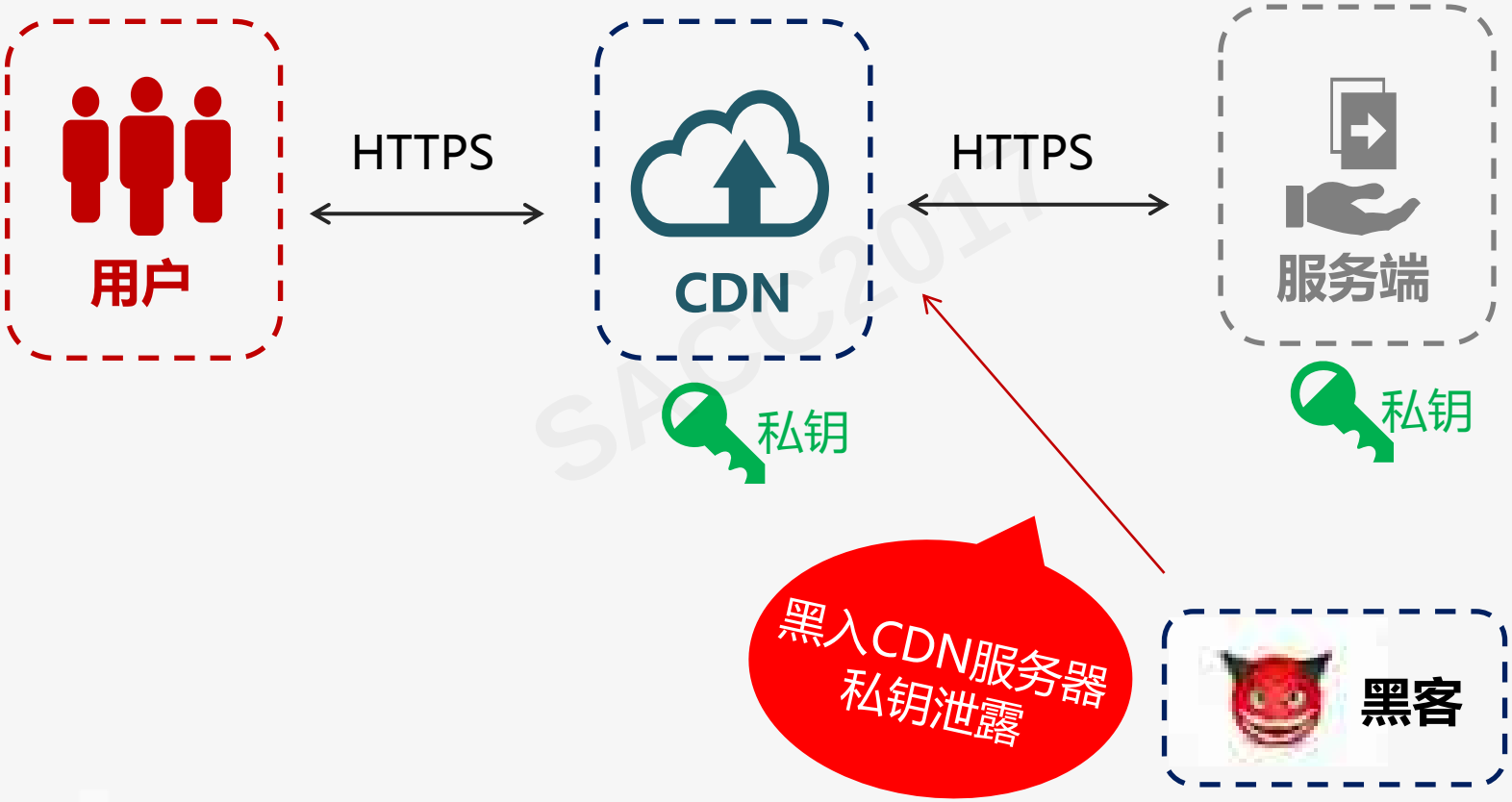
如何处理CDN/云上的私钥？



SACC2017

如何处理商用CDN上的私钥？

- 主动提供私钥给商用CDN厂商（HTTPS不再安全）



SACC2017

Keyless解决方案

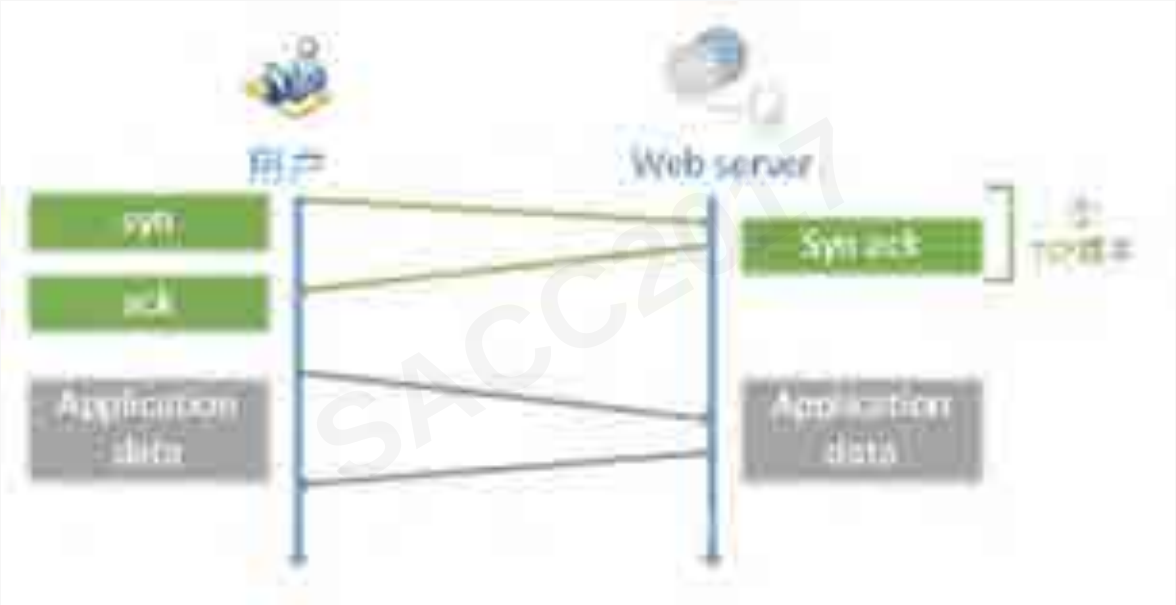
适用于金融，提供一台实时计算的 Key Server 。CDN 要用到私钥时，通过加密通道将必要的参数传给 Key Server，由 Key Server 算出结果并返回即可。

https://github.com/cloudflare/keyless

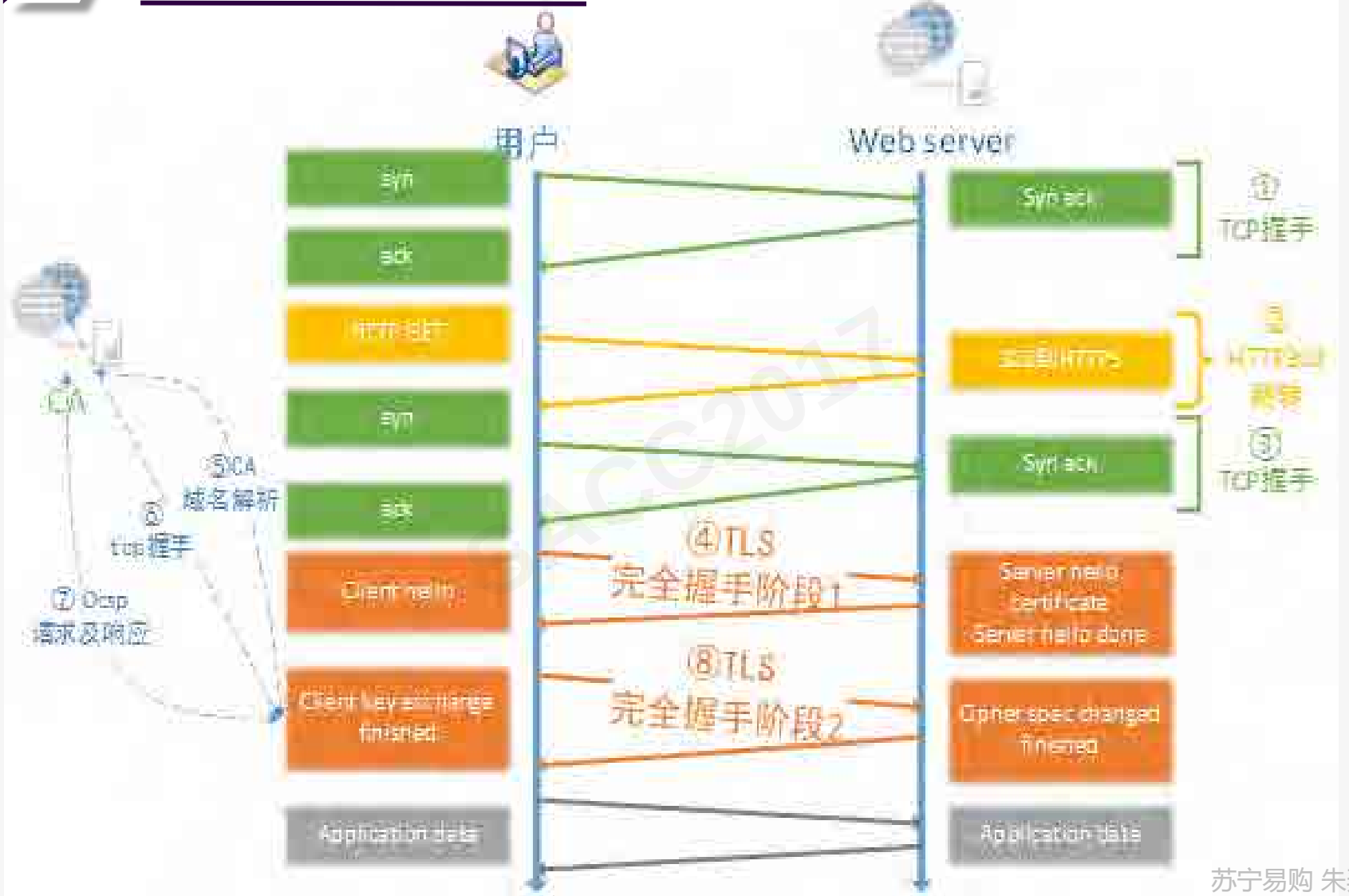
04

HTTPS性能优化篇

基本的HTTP请求


用户
Web server
syn
ack
Application data
Syn ack
Application data

客户端增加了传输延时



苏宁易购 朱羿全

服务端的额外开销增加了CPU的损耗

测试场景：HTTP首页	CPU资源消耗	设备资源消耗			性能指标		时间
并发用户	Varnish	平均CPU	最大CPU	吞吐量	TPS	响应时间	
100Vuser（4台测试机）	16%	17%	33%	1.5G	6133	0.015	02:39-02:54
100Vuser（23台测试机）	30%	18.20%	32%	2.2G	13009	0.008	03:33-03:41
200Vuser（23台测试机）	30%	18.20%	32%	2.3G	13068	0.015	03:42-03:47

测试场景：HTTP首页	CPU资源消耗	设备资源消耗			性能指标		时间
并发用户	Varnish	平均CPU	最大CPU	吞吐量	TPS	响应时间	
100Vuser（12台测试机）	26%	18.40%	35.80%	2.1G	9950	0.01	03:07-03:15
100Vuser（23台测试机）	32%	19.70%	34.30%	2.2G	12100	0.008	03:48-03:52
200Vuser（23台测试机）	32%	20.20%	34.10%	2.4G	13096	0.015	03:16-03:27

HSTS的合理使用

Strict-Transport-Security：max-age=expireTime [; includeSubDomains] [; preload]

优势

HSTS表明网站已经实现了TLS，要求浏览器对用户明文访问的Url重写成HTTPS，避免了始终强制302重定向的延时开销。

缺点

1. HSTS在max-age过期时间内在客户端是强制HTTPS的，服务端无法控制。因此，需要降级时，HTTPS无法及时切换到HTTP。
2. HSTS是严格的HTTPS，一旦网络证书错误时，网页将直接无法访问（用户无法选择忽视）。

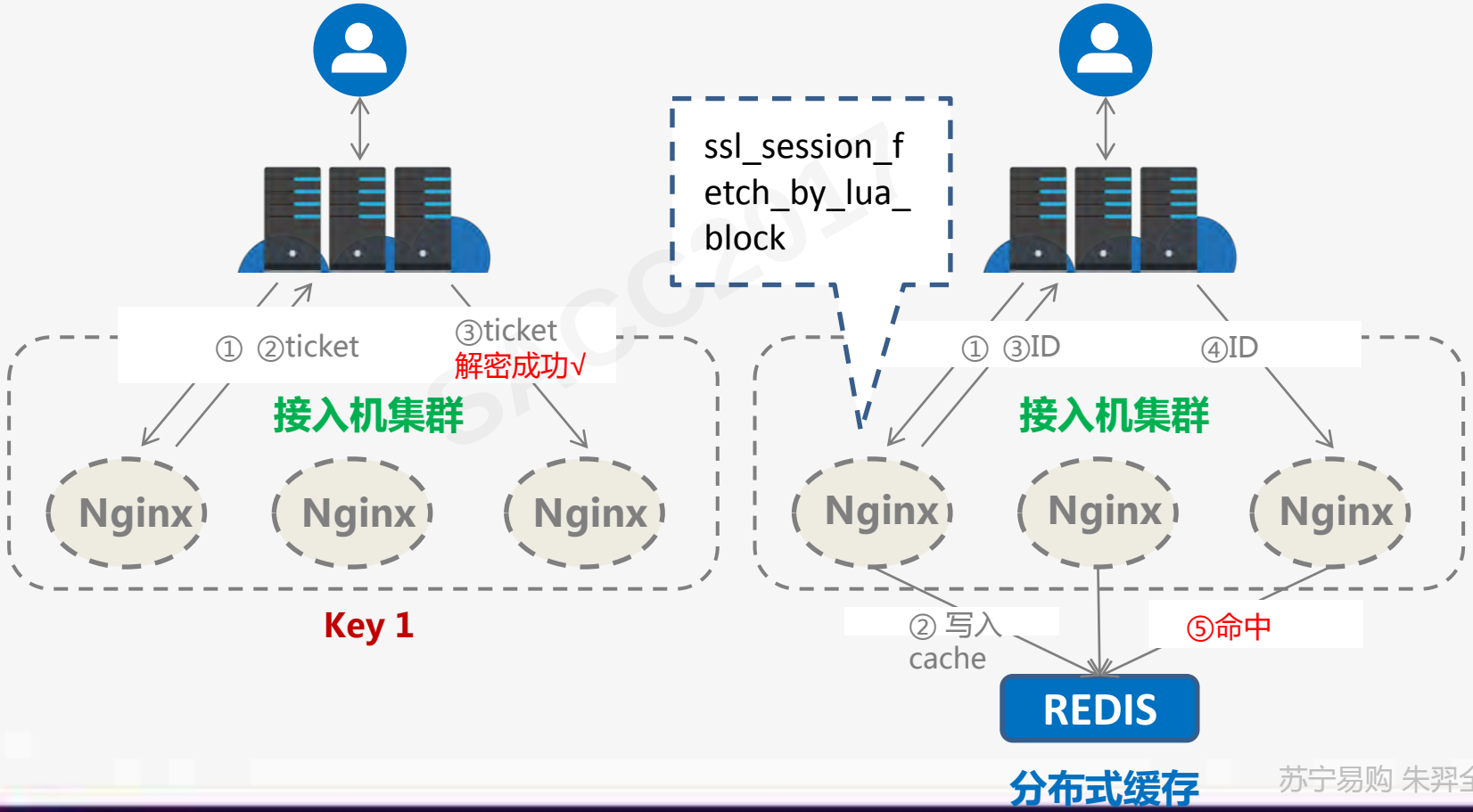
会话恢复的合理使用

会话恢复机制是指在一次完整协商的连接断开时，客户端和服务端会将会话的安全参数保存一段时间。后续的连接，双方使用简单握手恢复之前协商的会话。大大减少了TLS握手的开销。

会话恢复的方案可以分为两种：

会话ID（Session ID）：服务端缓存会话信息

会话票证（Session Ticket）：客户端缓存会话信息



Ocsp stapling的合理使用

OCSP（Online Certificate Status Protocol, 在线证书状态协议）用于查询证书的吊销信息。

OCSP stapling服务端可以代替客户端完成证书吊销状态的检测。

```
# 启用OCSP staplingssl_stapling on;
# valid表示缓存5分钟，resolver_timeout表示网络超时时间
resolver 8.8.8.8 8.8.4.4 223.5.5.5 valid=300s;resolver_timeout 5s;
 # 启用OCSP响应验证，OCSP信息响应适用的证书
ssl_stapling_verify on;
ssl_trusted_certificate /usr/local/nginx/ssl_cert/trustchain.crt;
```

SACC 2017

TLS协议的合理配置

1.指定TLS协议的版本，不安全的SSL2和SSL3要废弃掉

2.启用ssl_prefer_server_ciphers，用来告诉Nginx在TLS握手时启用服务器算法优先

3.选择最优的加密套件以及优先顺序，具体可参考Mozilla的https://wiki.mozilla.org/Security/Server_Side_TLS

4.如果有双向验证的需求，可以开启Nginx的客户端身份验证

```
# 要求客户端身份验证
ssl_verify_client on;
# 指定客户端证书到根证书的最大证书路径长度
ssl_verify_depth 3;
# 指定允许签发客户端证书的CA证书
ssl_client_certificate trustchain.crt;
# 完整证书链中需要包含的其他CA证书
ssl_trusted_certificate root-ca.crt;
# 证书吊销列表
ssl_crl revoked-certificates.crl;
```

SACC2017

SNI功能的合理使用

SNI（Server Name Indicate）允许客户端在发起SSL握手请求时（ClientHello阶段），就提交请求的Host信息，使得服务器能够切换到正确的域并返回相应的证书。通过这种方式解决了一个IP（虚拟机）部署多个域名服务的问题。

Nginx支持SNI的方式并自动开启。

```
server {
        listen 443 ssl default_server;
        ssl_certificate
        /usr/local/nginx/cert/serversuning.pem;
        ssl_certificate_key
        /usr/local/nginx/cert/suning.key;
        ...
}
server {
        listen 443 ssl;
        server_name sit1.suning.com;
        ssl_certificate
        /usr/local/nginx/cert/serversuningcom.pem;
        ssl_certificate_key
        /usr/local/nginx/cert/suningcom.key;
        ...
}
server {
        listen 443 ssl default_server;
        server_name sit1.suning.cn;
        ssl_certificate
        /usr/local/nginx/waf/serversuningcn.pem;
        ssl_certificate_key
        /usr/local/nginx/waf/suningcn.key;
        ...
}
```

SACC2017

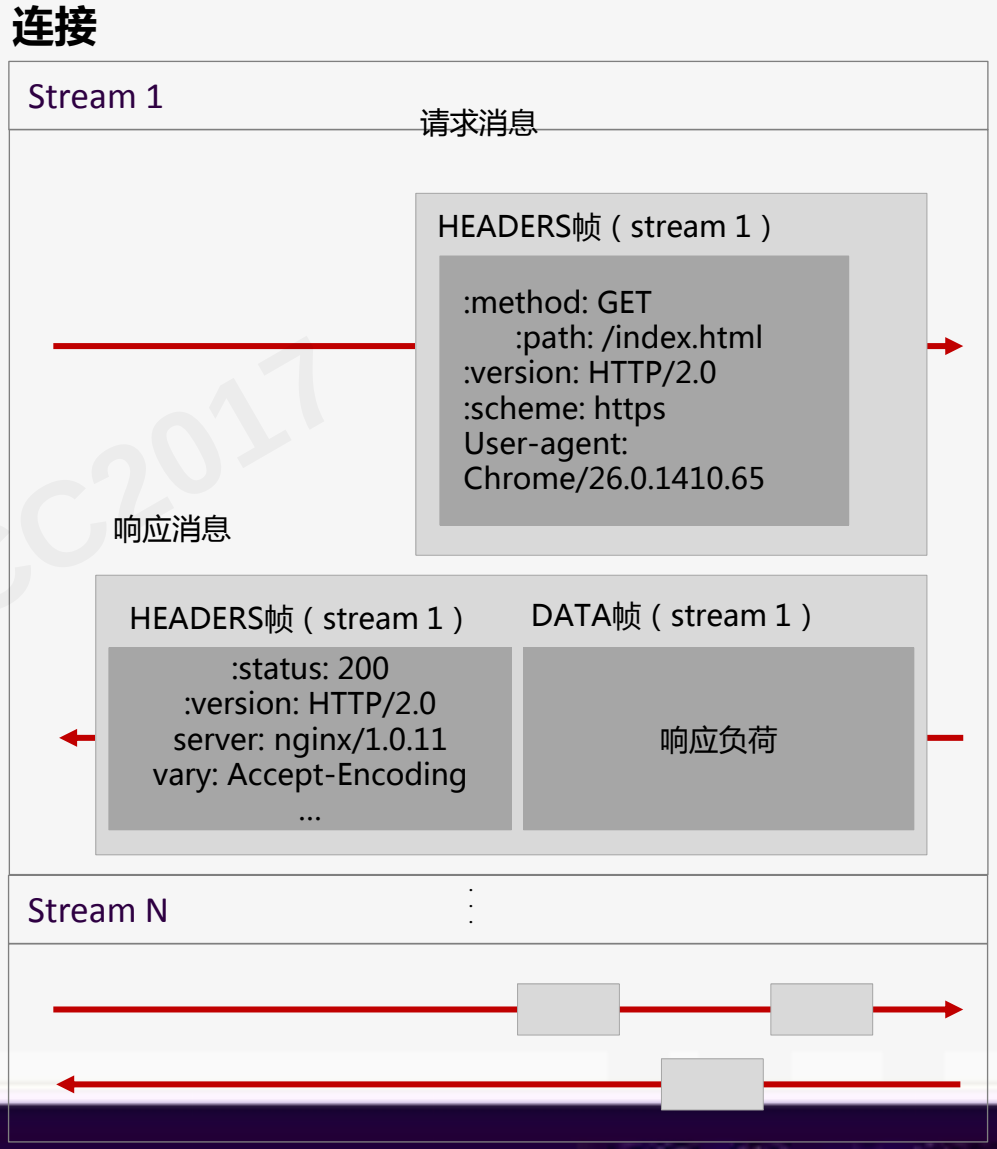
HTTP/2&QUIC的合理使用——HTTP/2

帧（frame）： HTTP 2.0通信的最小单位，包括帧首部、流标识符、优先值和帧净荷等。

消息（message）：是指逻辑上的HTTP消息（请求/响应）。一系列数据帧组成了一个完整的消息。比如一系列DATA帧和一个HEADERS帧组成了请求消息。

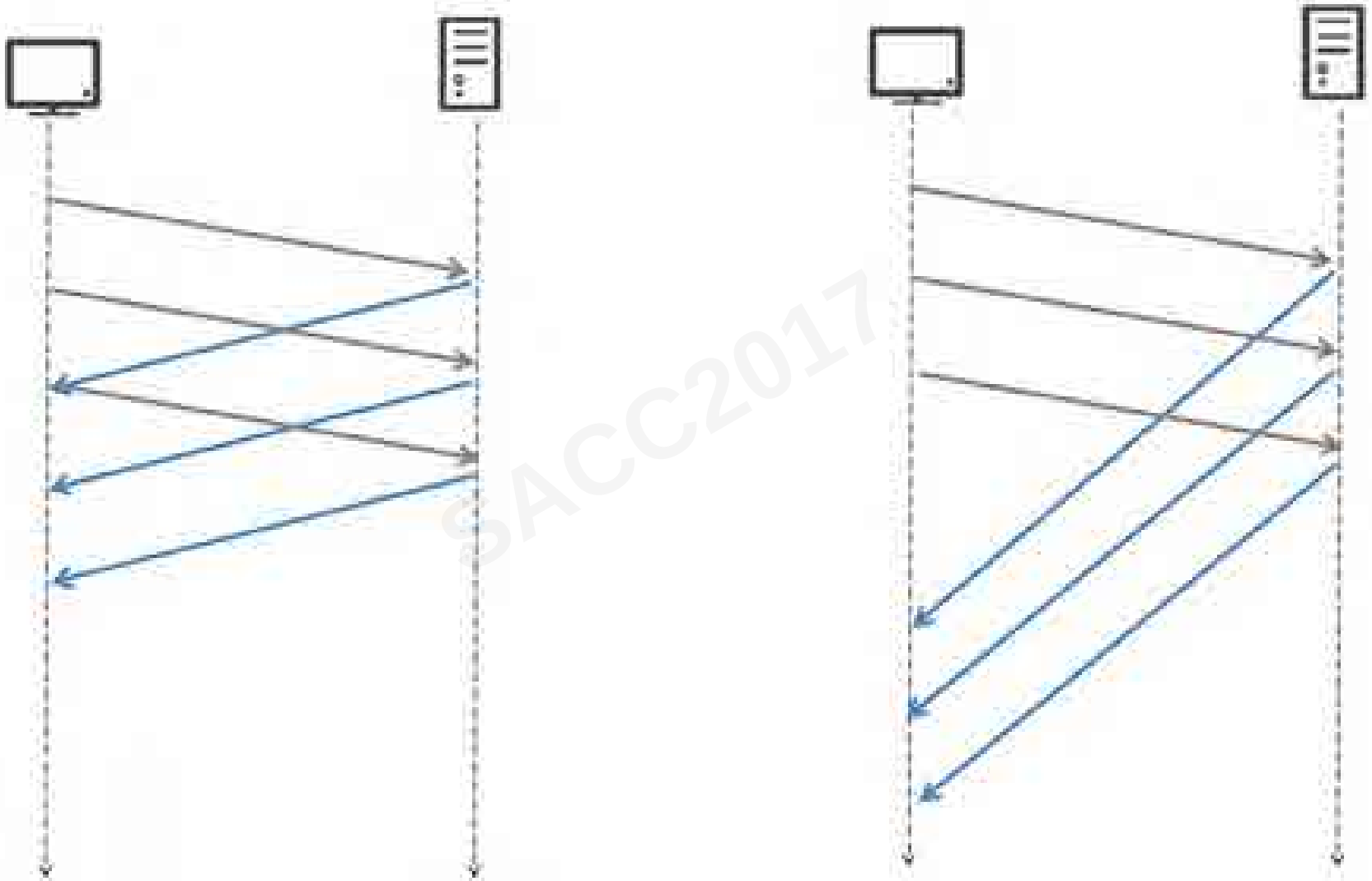
流（stream）：流是连接中的一个虚拟信道，可以承载双向消息传输。每个流有唯一整数标识符。为了防止两端流ID冲突，客户端发起的流具有奇数ID，服务器端发起的流具有偶数ID。

每个数据流以 消息的形式发送， 而消息由一或多个帧组成， 这些帧可以乱序发送， 然后根据每个帧首部的流标识符重新组装。



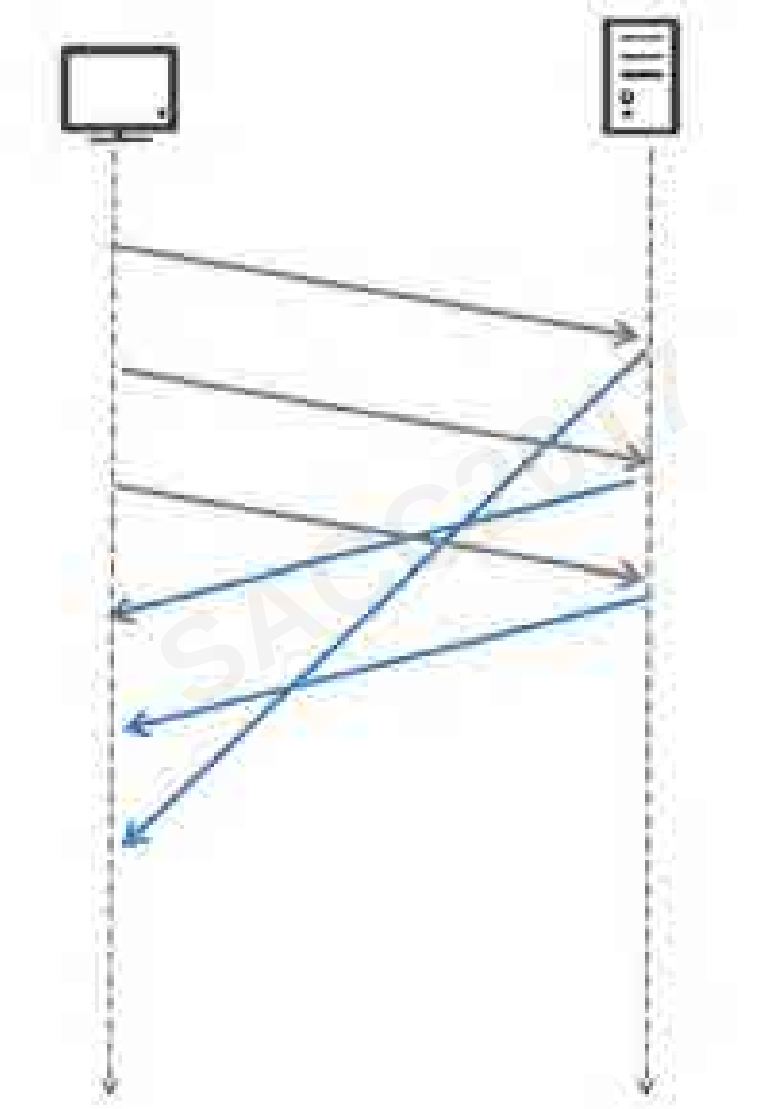
SACC2017

HTTP/2&QUIC的合理使用——HTTP/2



SACC2017

HTTP/2&QUIC的合理使用——HTTP/2



HTTP/2&QUIC的合理使用——HTTP/2优点

多路复用共享连接

请求优先级

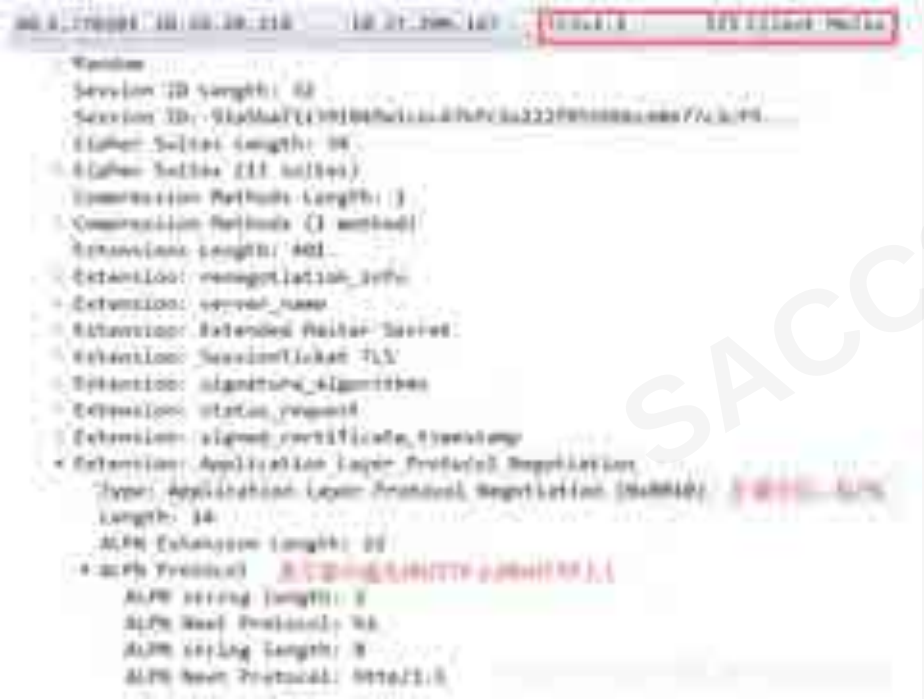
服务端推送

首部压缩

SACC2017

HTTP/2&QUIC的合理使用——HTTP/2

基于ALPN的协商过程



SACC2017

ngx_http_v2_module模块安装

(1) 配置

```
./configure --with-http_ssl_module \
        --with-http_v2_module \
        --with-debug \
        --with-openssl=/path/to/openssl-1.0.2
```

(2) 编译并安装

```
make&make install
```

(3) 修改nginx.conf配置

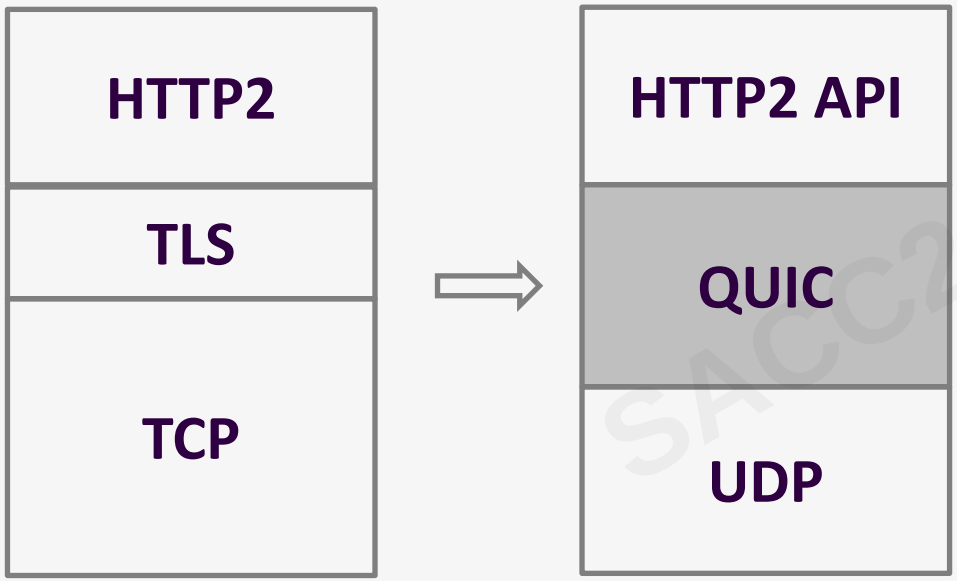
```
server {
        listen 443 default_server ssl http2;

        ssl_certificate       server.crt;
        ssl_certificate_key   server.key;

        ...
}
```

SACC2017

HTTP/2&QUIC的合理使用——QUIC



问题：

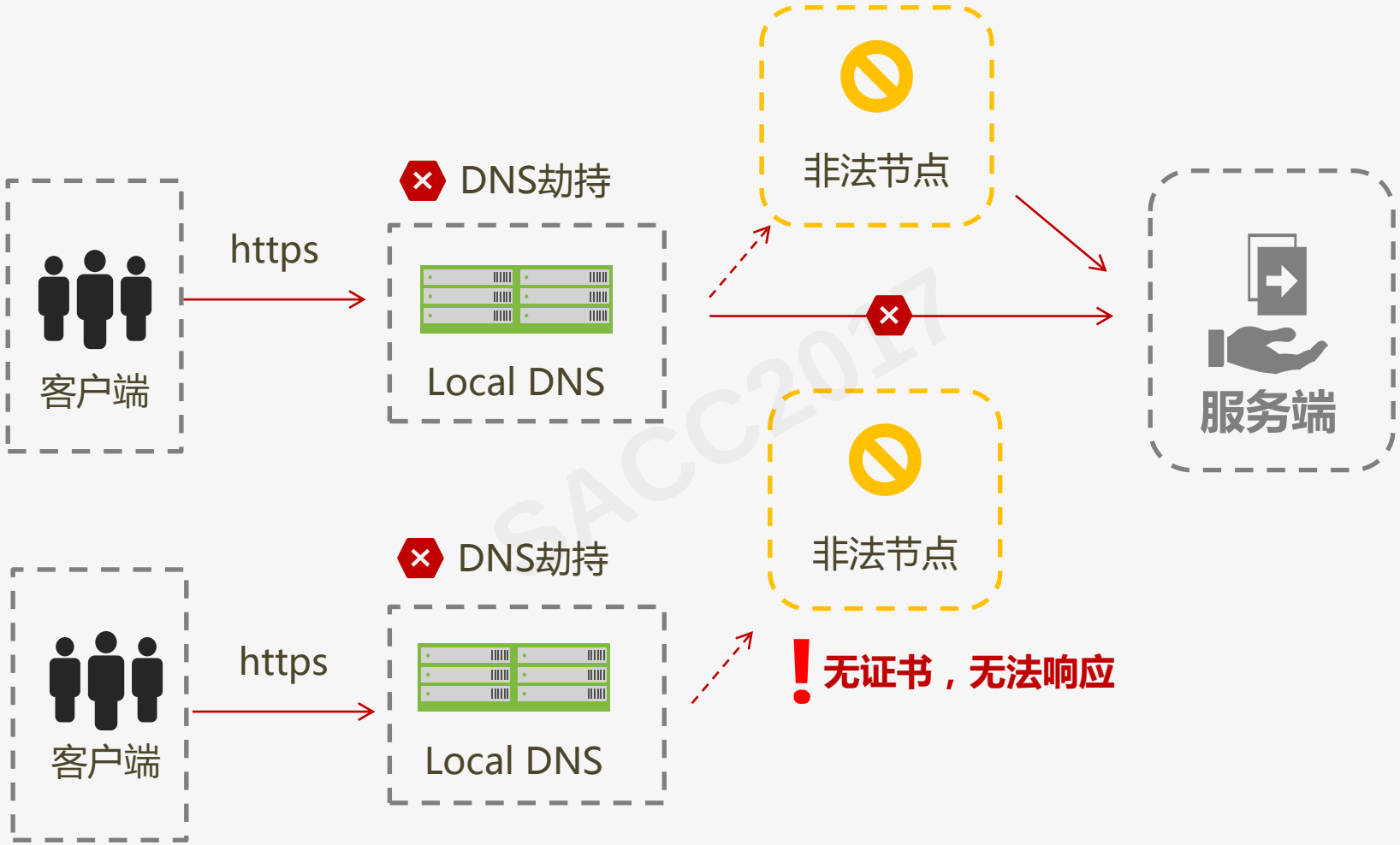
1.缺乏稳定服务端容器支持，目前caddy

2.缺乏客户端支持，目前只有Chrome

3.复杂网络环境下udp诸多限制

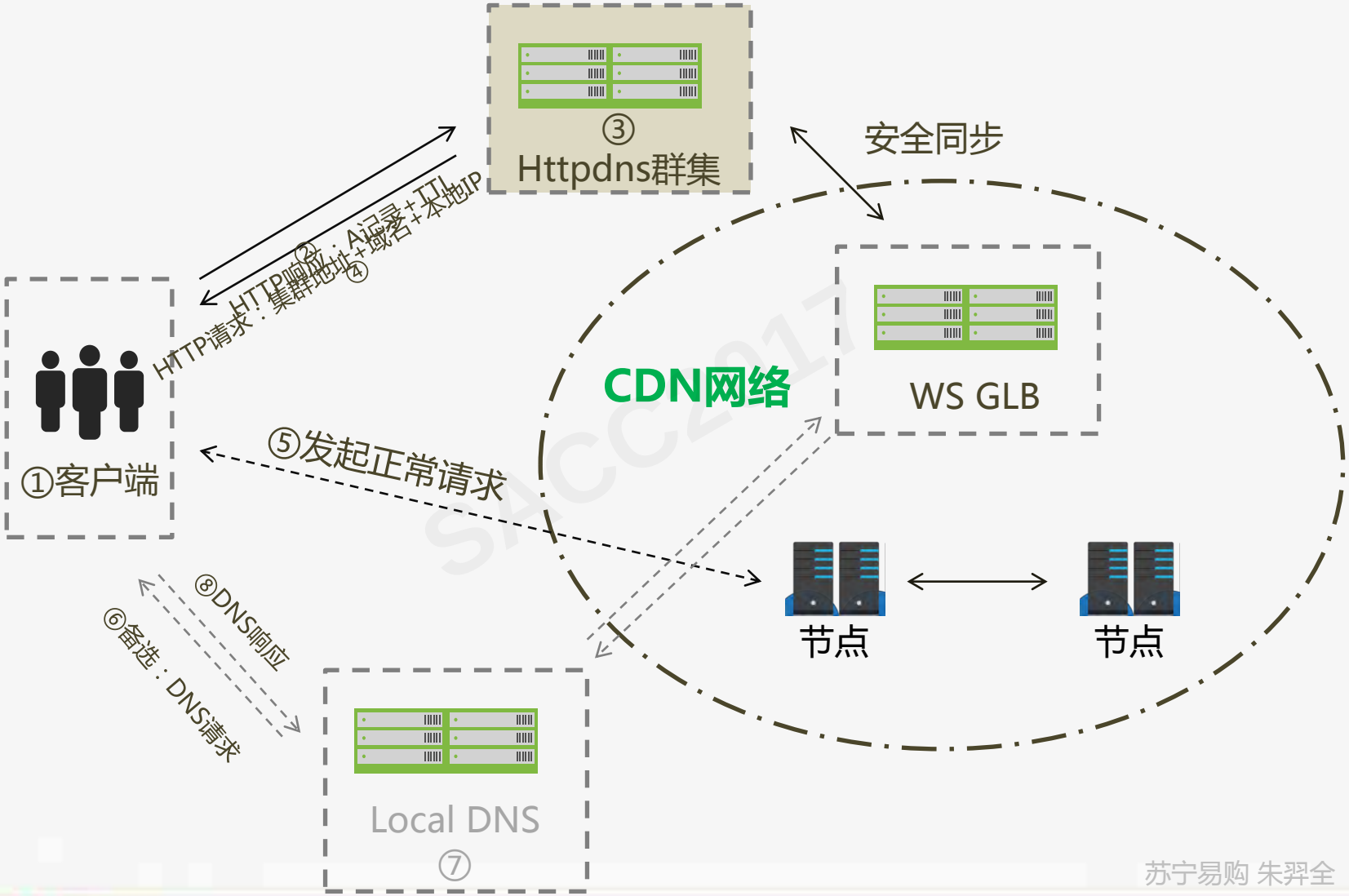
SACC2017

- HTTPS使DNS劫持问题扩大化



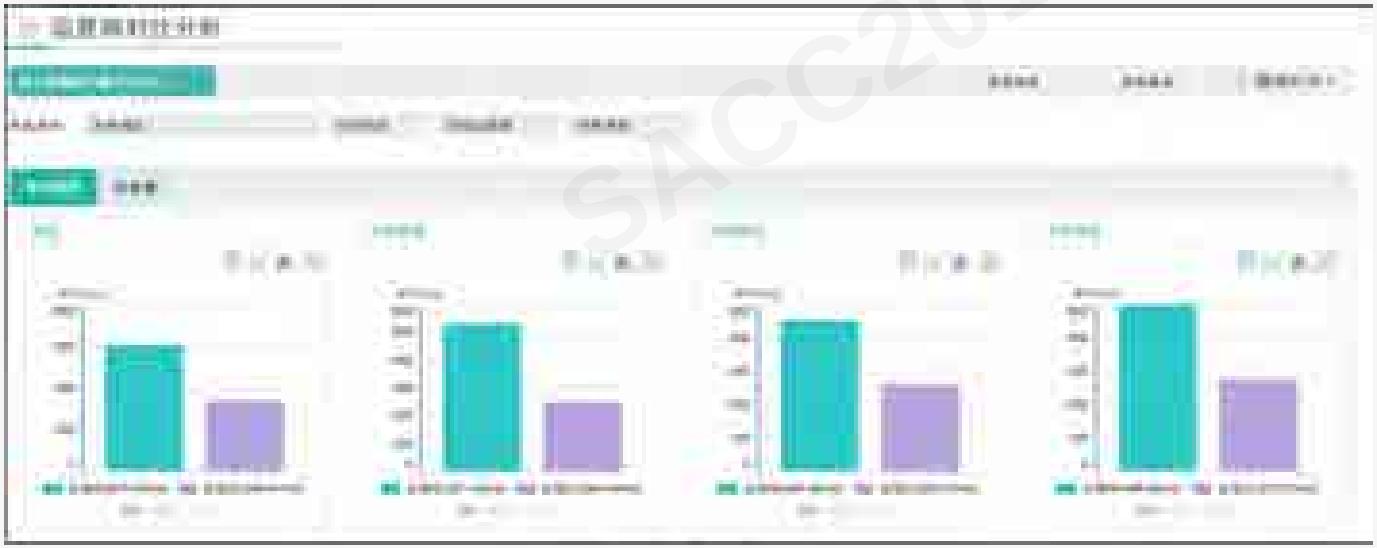
SACC2017

- HttpDNS 解决 DNS攻击劫持



SACC2017

安卓 加速效果对比



IOS 加速效果对比

SACC2017

05

HTTPS灰度上线篇

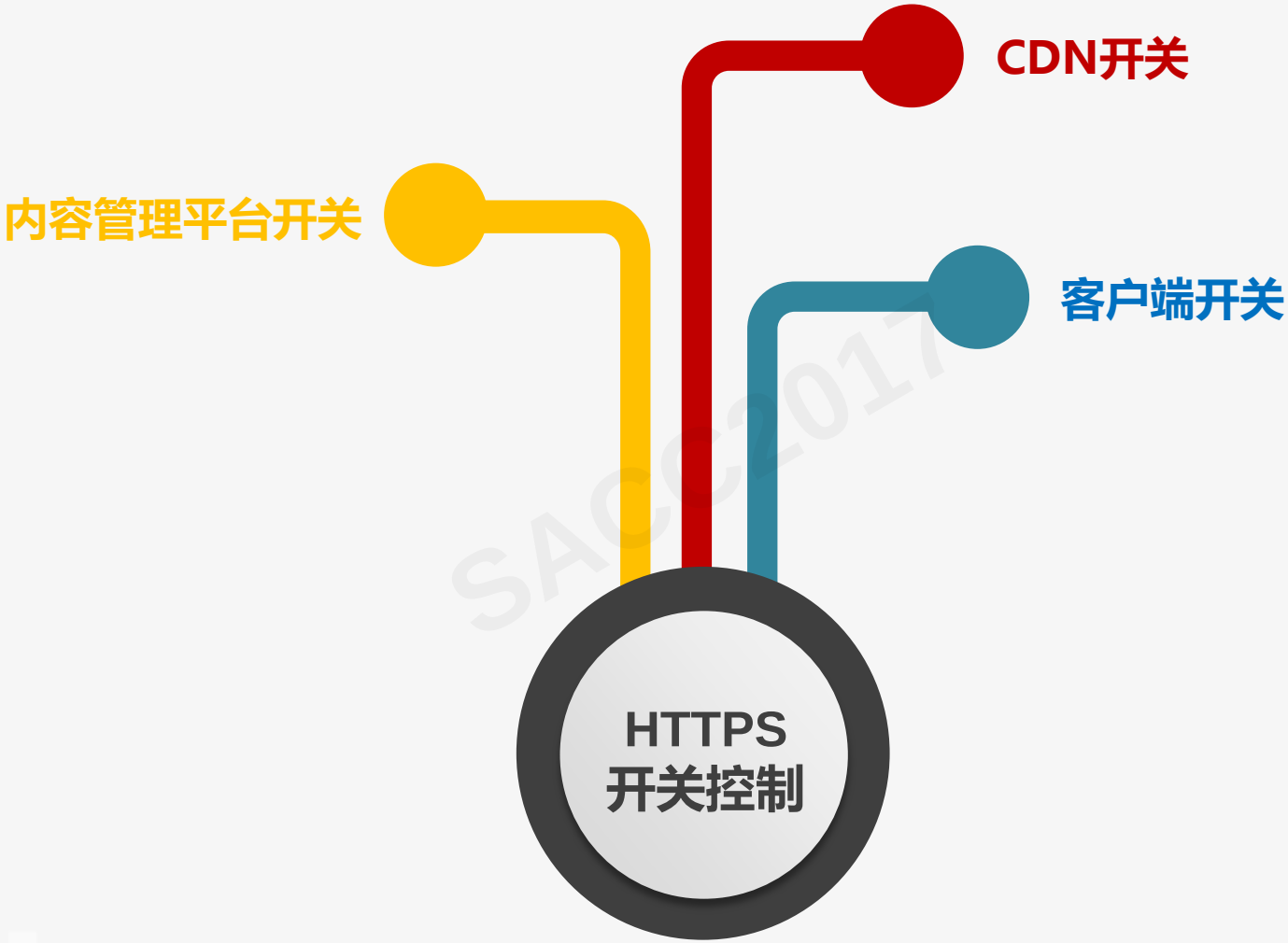
HTTPS上线

原则

- 灰度原则
- 降级原则
- 开闭原则

苏宁易购 朱洋全

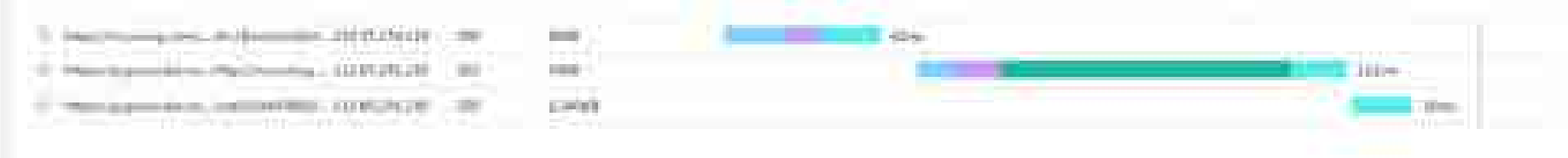
HTTPS开关控制



SACC2017

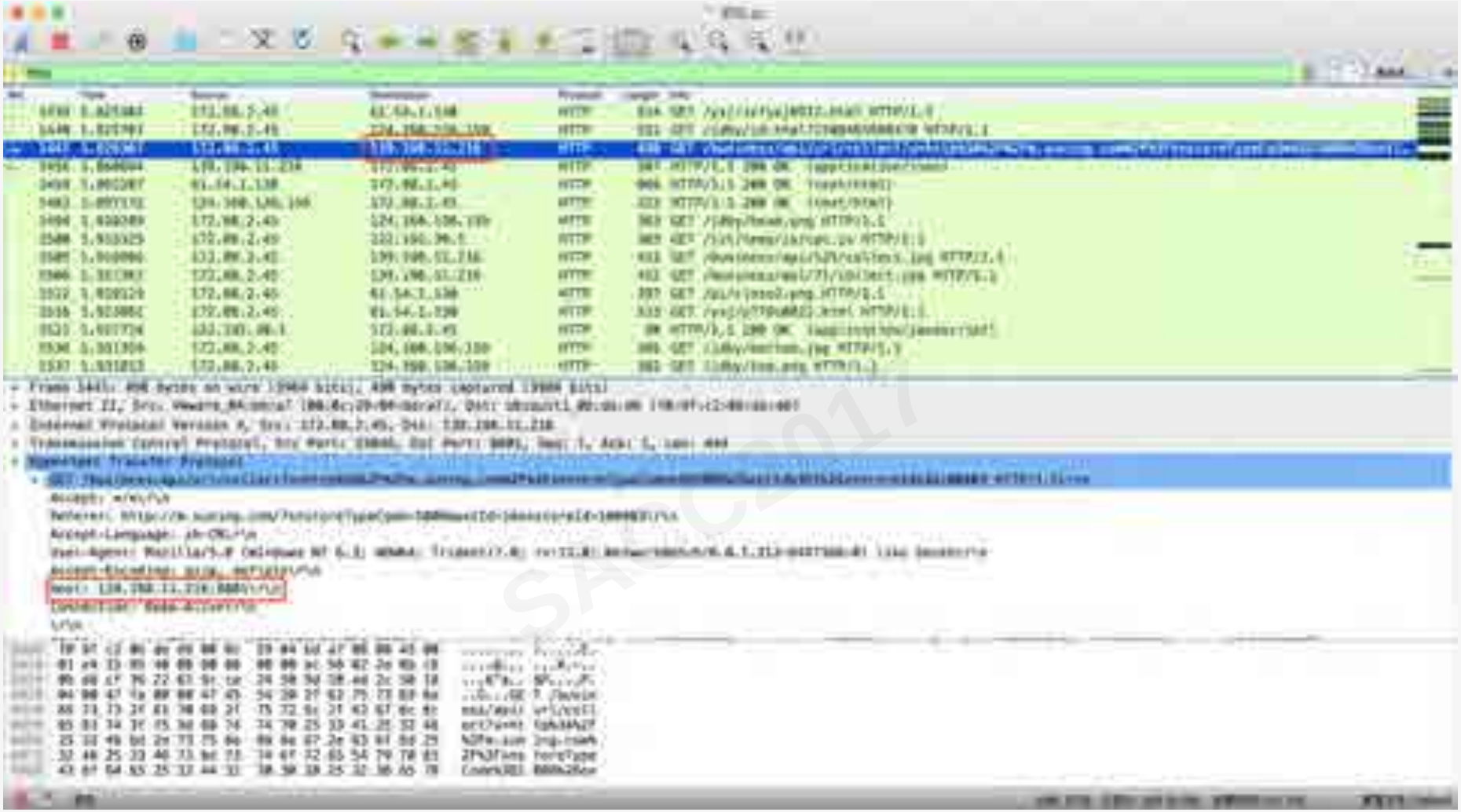
HTTPS性能监控

苏宁易购 朱羿全



SACC2017

苏宁易购 朱羿全



SASC 2017 云智慧 9

THANKS