FIG 1

1
Client
2
12
Router
11a
HTTP-Proxy
(Transparent)
Firewall
11b
HTTP-Proxy
(Transparent)
11c
HTTP-Proxy
(Transparent)
https
3
Web-HTTP
Server
4
Web-Application
Server
http
5
Central Location
Lookup Server

FIG 2

6
8
6a
6b
6c
6d
163.52.128.72 (IP address client A)→ CH
175.63.228.79 (IP address client B)→ ES
219.32.119.03 (IP address client C)→ US
135.63.728.12 (IP address client D)→ CH
8a
8b
8c
8d
7

4
Web-Application Server
5
Central Location Lookup Server
4a
Web Application
Location (e.g. GB)
3
3a
3c
Web Server https 443
LLS Plugin
Public Key
Location Lookup Service
Private Key
5b
IP-Lookup File or DB
7a
5a
Web Server http 80
100
Network Infrastructure
1.
4.
2.
3.
2
Client

FIG 3

FIG 4

Browser (Client)
WebServer
WebServer LLS-Plugin
LLS
WebApplication
2a
3
3a
5
4a
user
clicks URL
A
https request (SSL)
B
request
C
redirect to LLS
D
C1
location (country) not in session yet
generate random key (llrk)
C2
D
redirect to LLS
D
http request (no SSL)
D
E
lookup / sign location
redirect to initial website (signed token)
F
request (signed token)
F
F
request (signed token)
G
verify signature/store location in session
redirect (no token)
H
redirect (no token)
H
https request (SSL)
H
request
H
response
L
response
L
response
L
I
add header X-Auth-Location
K
response
L
show content
L
user