THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

THE OHIO STATE UNIVERSITY

Personalized Pseudonyms for Servers in the Cloud

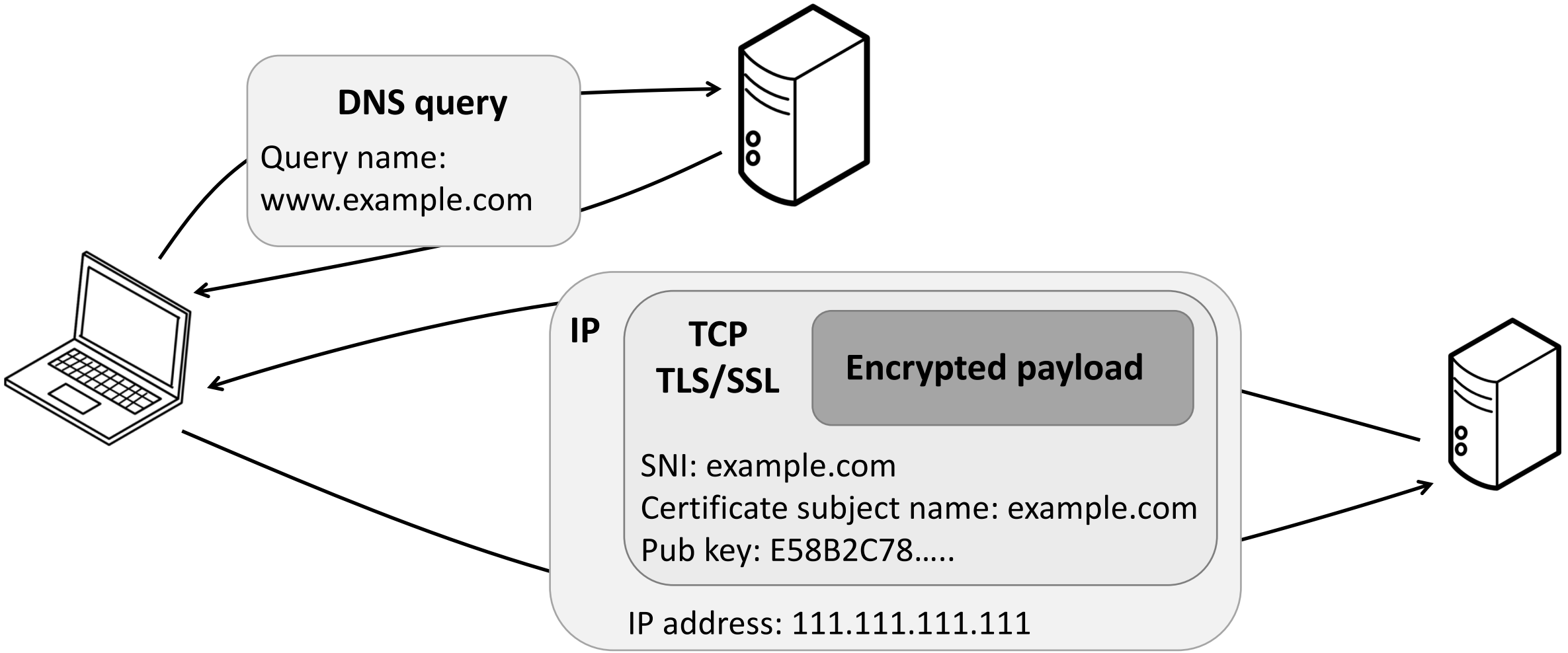
Qiuyu Xiao (UNC-Chapel Hill)

Michael K. Reiter (UNC-Chapel Hill)

Yinqian Zhang (Ohio State Univ.)

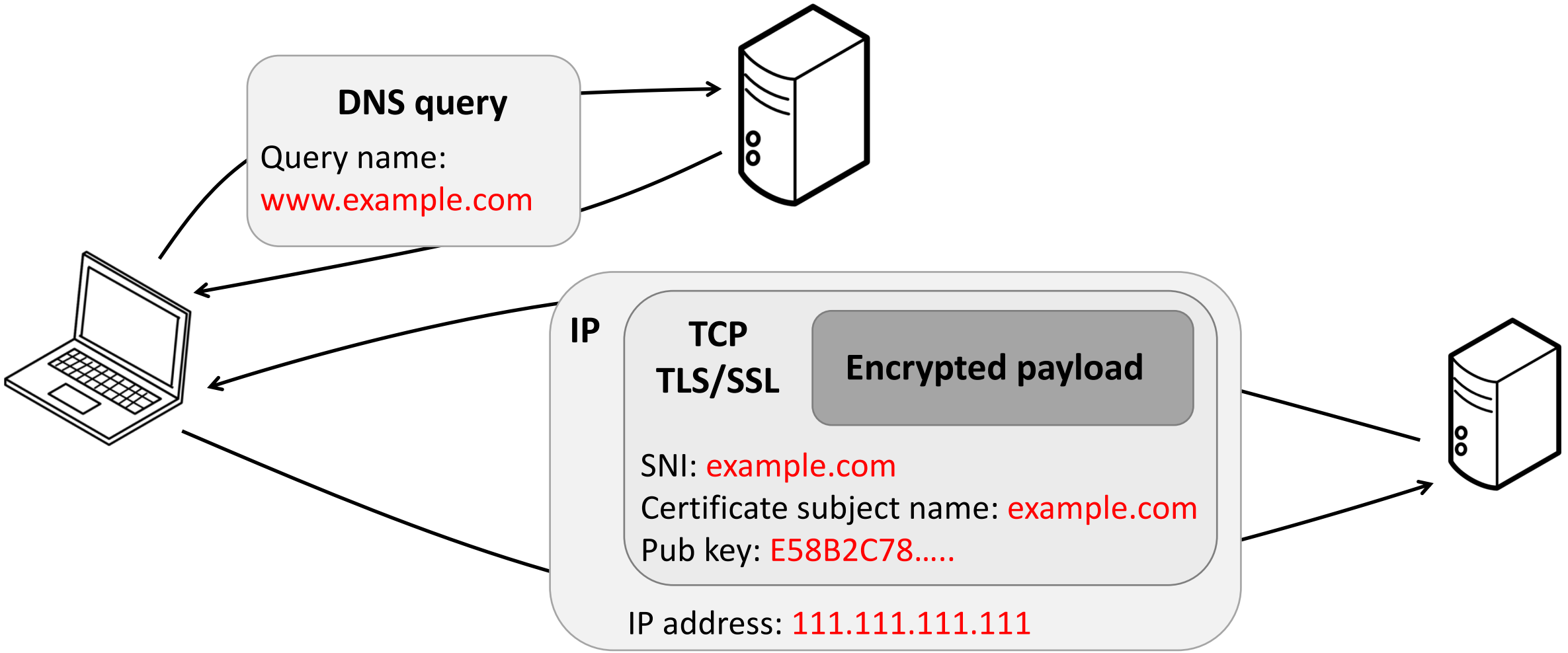
Background

Server's identity is not well protected with the normal HTTPS connection.



Background

Server's identity is not well protected with the normal HTTPS connection.



Background

Real-world adversaries compromise user’s privacy.

Background

Real-world adversaries compromise user's privacy.


PAKISTANI COURT SENTENCES A MAN TO DEATH OVER FACEBOOK POSTS

Slate

future tense | THE CITIZEN'S GUIDE TO THE FUTURE | JUNE 15 2017 5:13 PM

Pakistani Court Sentences a Man to Death Over Facebook Posts

By Meeran Karim

151 0 44

Background

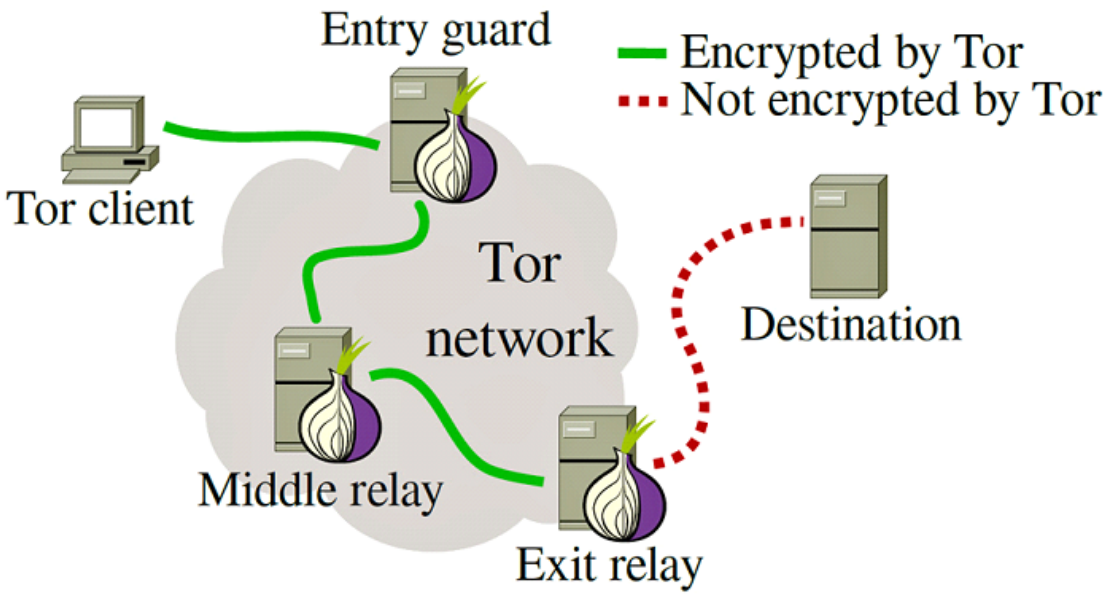
Real-world adversaries compromise user's privacy.

Existing solutions

- VPN tunneling
  - Encrypt and tunnel user's traffic through proxy server

Existing solutions

- Tor
  - Route encrypted packets through multiple Tor relays



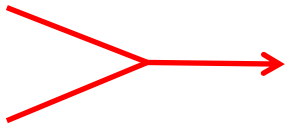
Existing solutions

- Cloud and CDN based solutions
  - CloudTransport[1]
  - Domain fronting[2]
  - CacheBrowser[3]

1. Cloud-Transport: Using cloud storage for censorship-resistant networking, PETS 2014
2. Blocking-resistant communication through domain fronting, PETS 2015
3. CacheBrowser: Bypassing Chinese censorship without proxies using cached content, CCS 2015

Existing solutions

- Cloud and CDN based solutions
  - CloudTransport[1]
  - Domain fronting[2]
  - CacheBrowser[3]



non-cooperative cloud provider

1. Cloud-Transport: Using cloud storage for censorship-resistant networking, PETS 2014
2. Blocking-resistant communication through domain fronting, PETS 2015
3. CacheBrowser: Bypassing Chinese censorship without proxies using cached content, CCS 2015

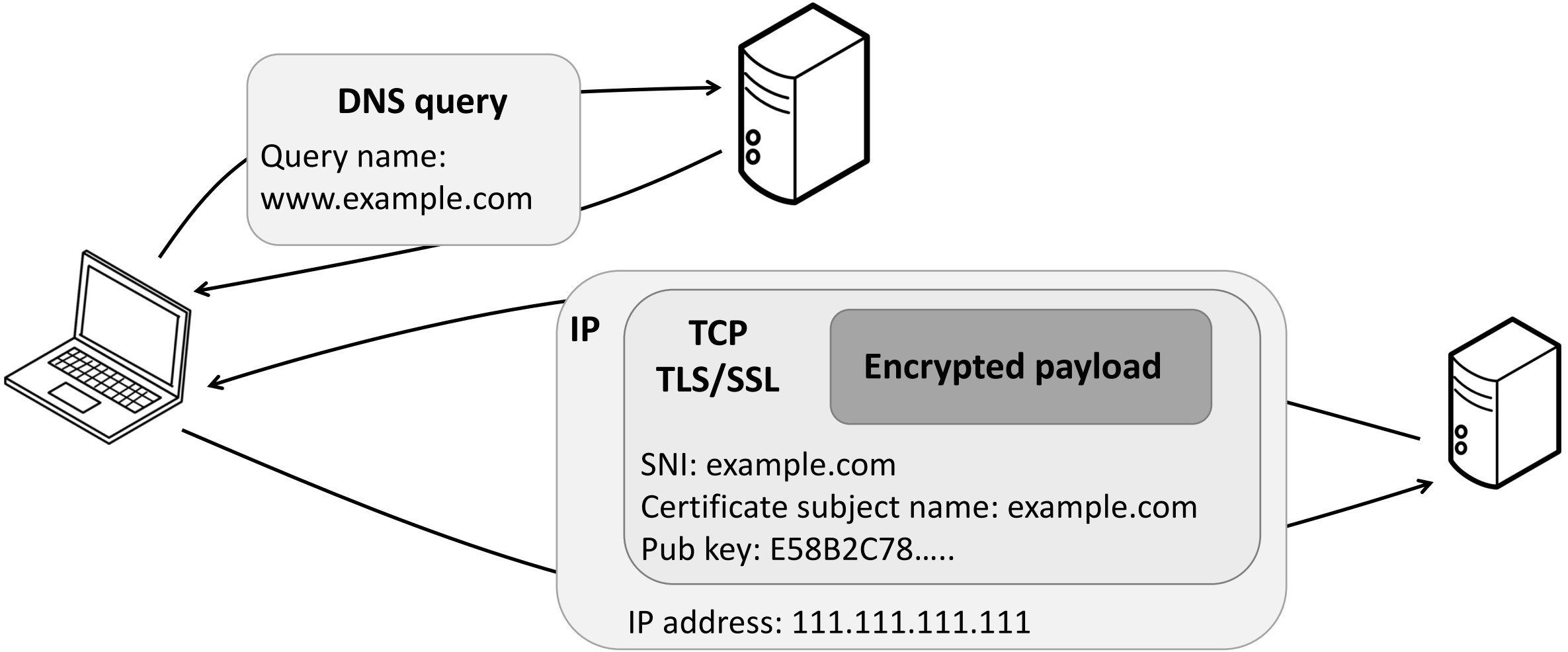
Existing solutions

- Cloud and CDN based solutions
  - CloudTransport[1]
  - Domain fronting[2]
  - CacheBrowser[3] ⟶ Domain name is visible in TLS SNI field

1. Cloud-Transport: Using cloud storage for censorship-resistant networking, PETS 2014
2. Blocking-resistant communication through domain fronting, PETS 2015
3. CacheBrowser: Bypassing Chinese censorship without proxies using cached content, CCS 2015

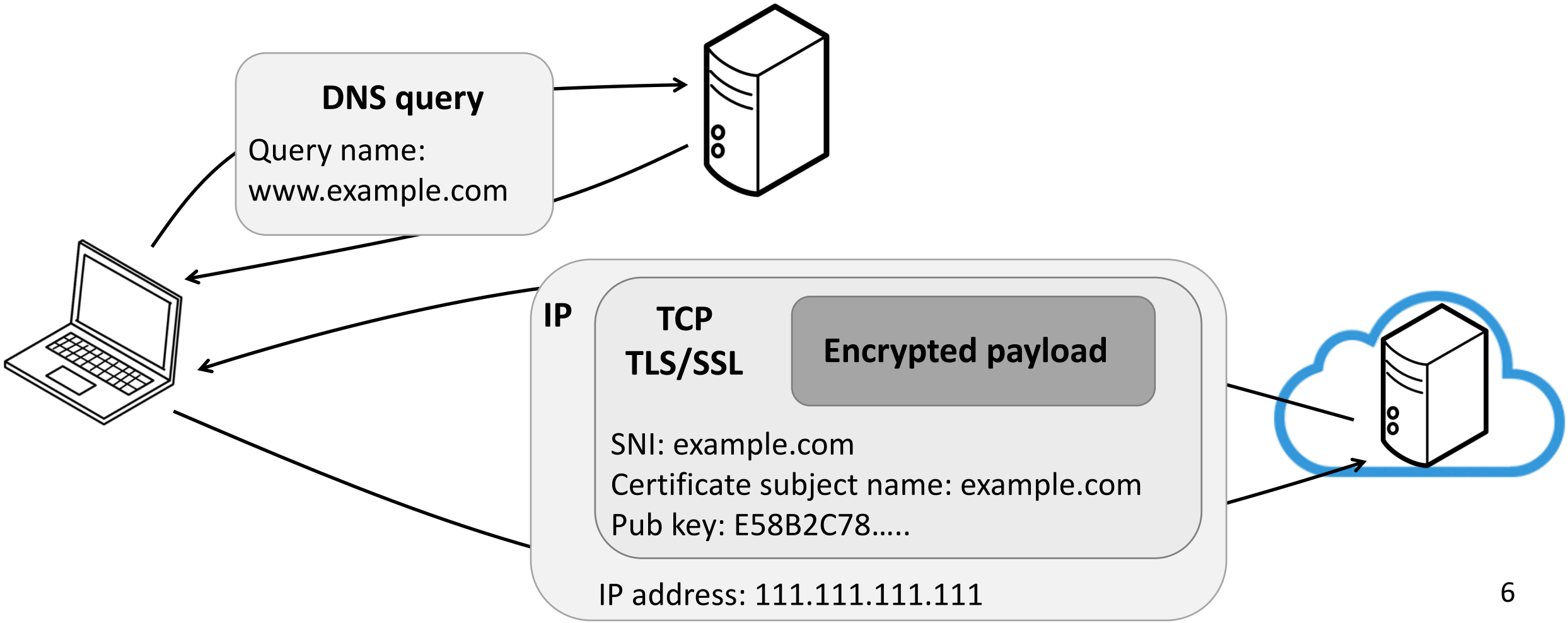
Our solution

Personalized Pseudonym for a Server in the Cloud (PoPSiCl)



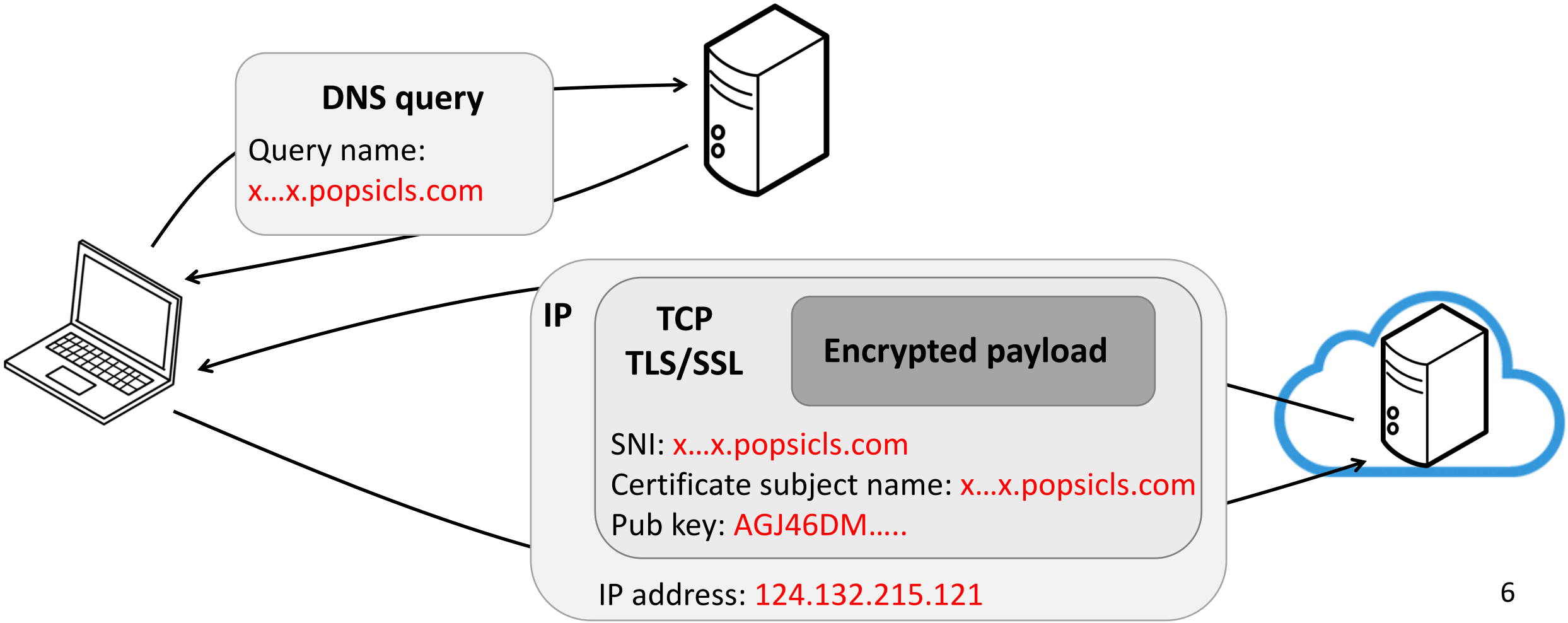
Our solution

Personalized Pseudonym for a Server in the Cloud (PoPSiCl)



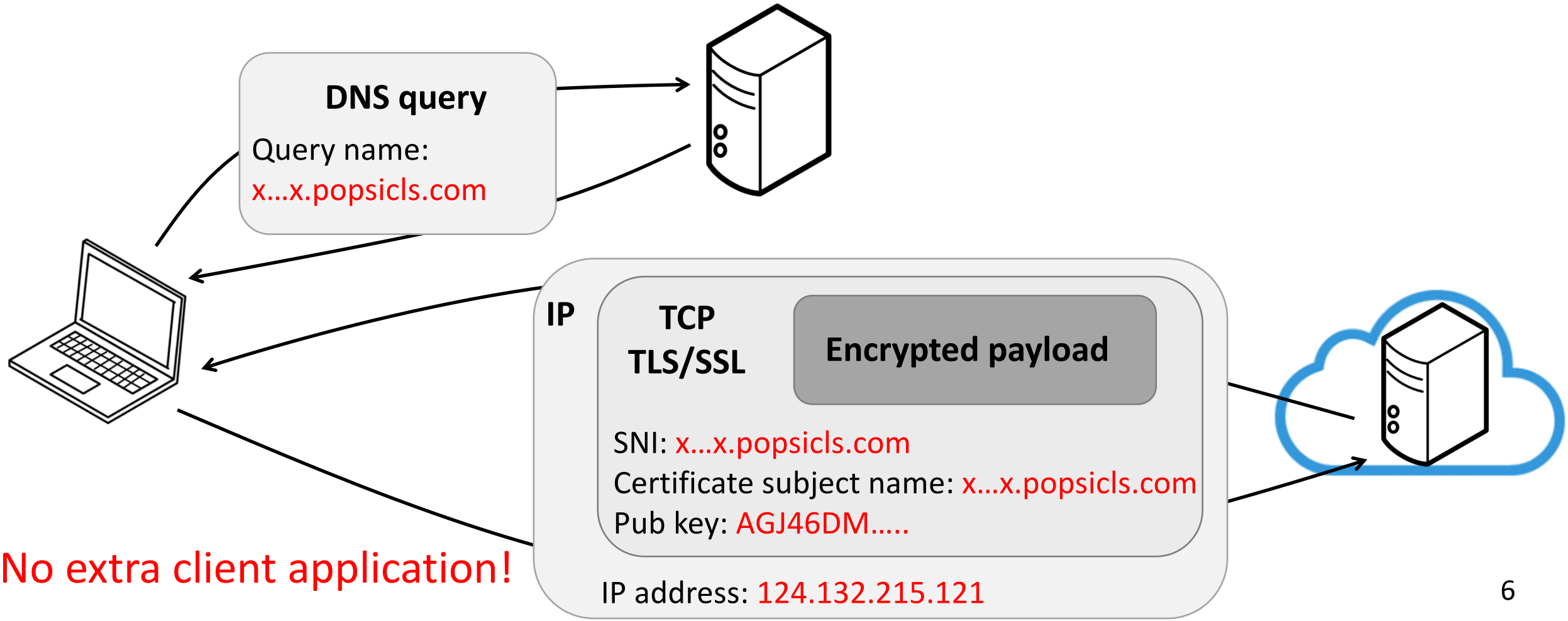
Our solution

Personalized Pseudonym for a Server in the Cloud (PoPSiCl)



Our solution

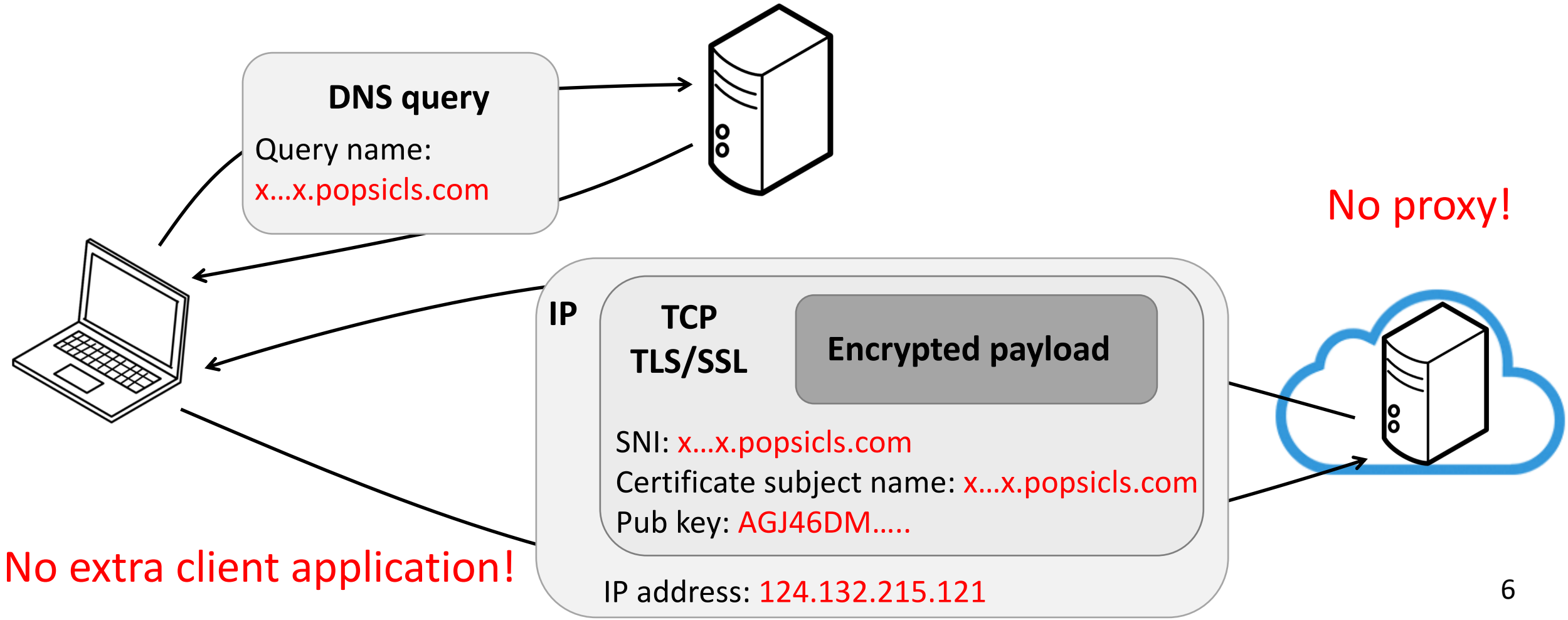
Personalized Pseudonym for a Server in the Cloud (PoPSiCl)



No extra client application!

Our solution

Personalized Pseudonym for a Server in the Cloud (PoPSiCl)



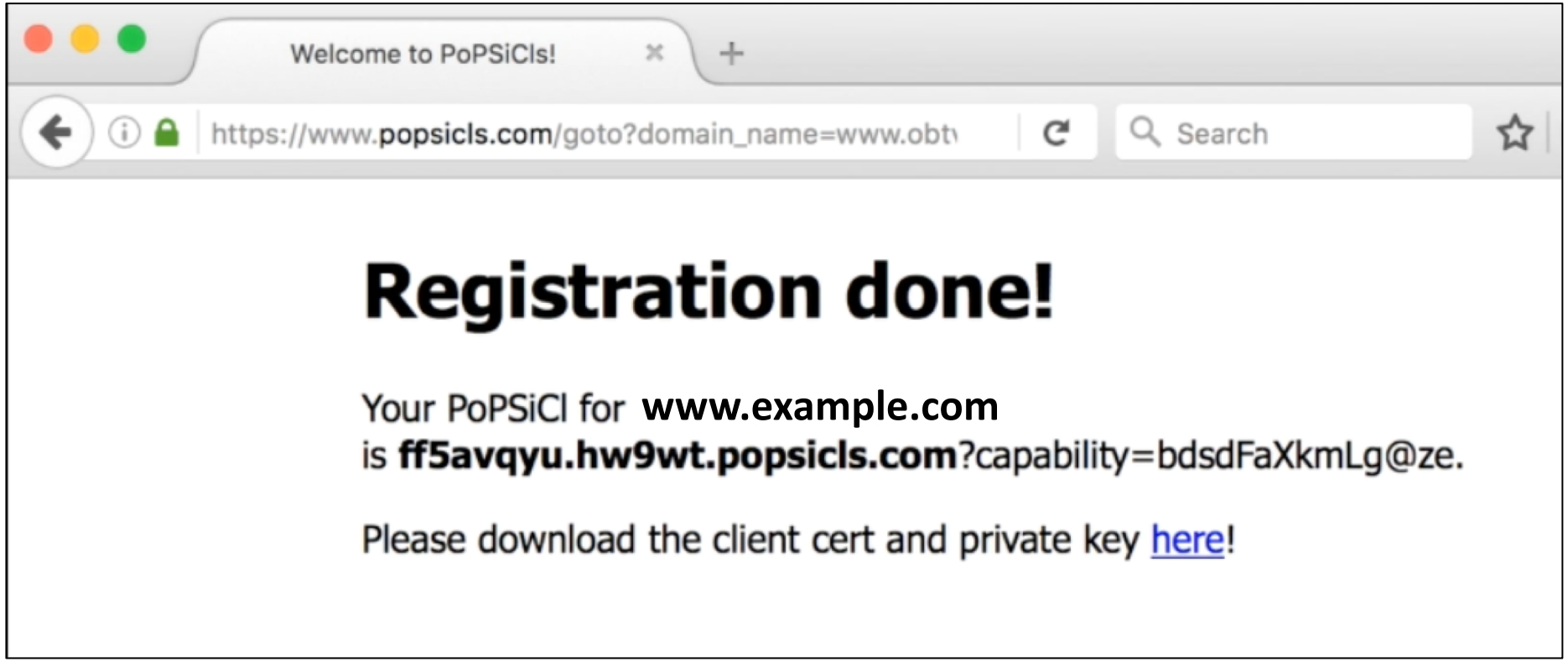
Threat model

In the context of a client-server interaction …

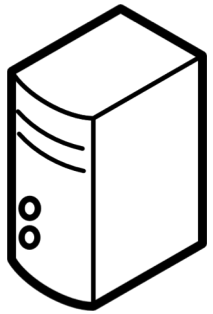
- What is trusted
  - Client computer
  - Cloud infrastructure (including the server computer)
- What is not trusted
  - The network between the client and the cloud
  - Other clients and other servers

PoPSiCl registration

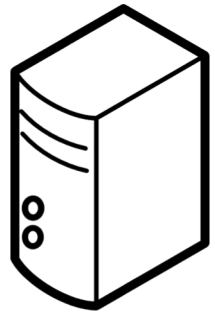
PoPSiCl registration



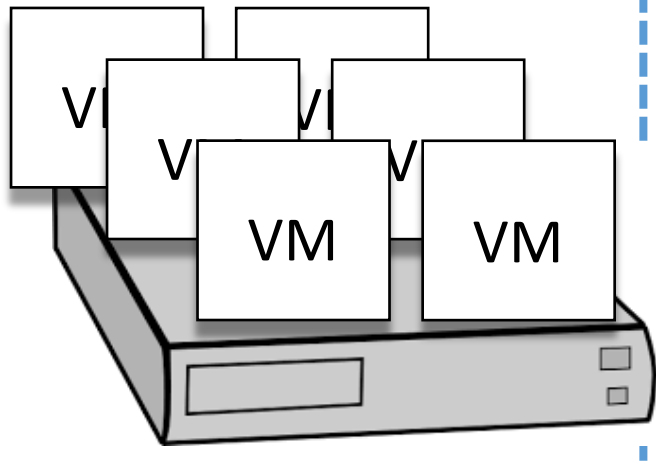
PoPSiCl registration

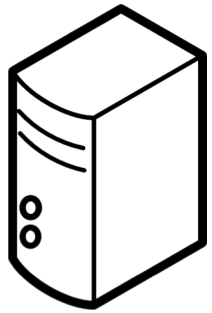


PoPSiCl store



DNS server



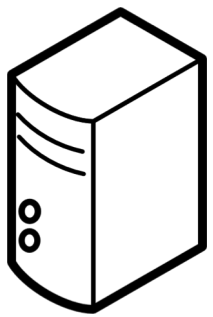


SDN controller

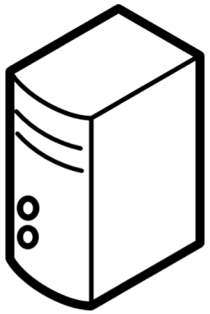
Cloud

PoPSiCl registration

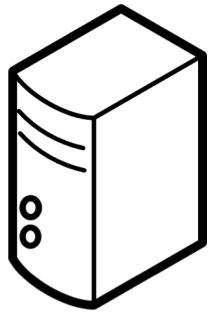
Registration request



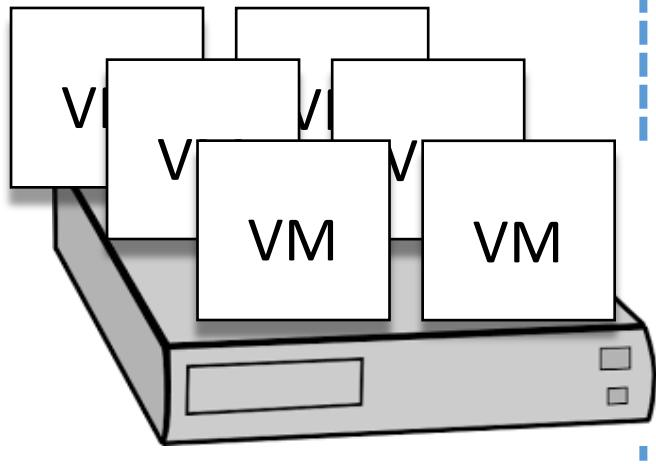
PoPSiCl store



DNS server



SDN controller

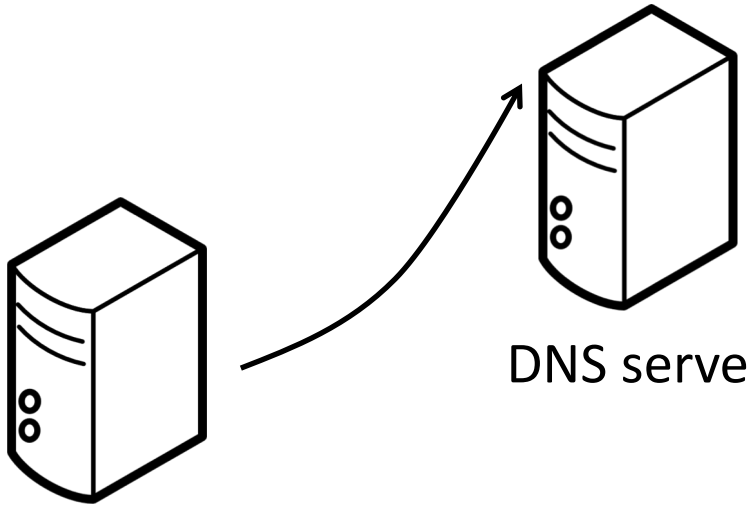


Cloud

PoPSiCl registration

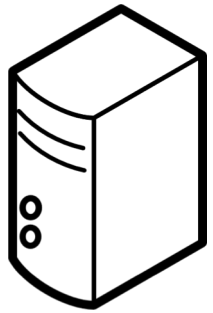
PoPSiCl

Pseudo IP

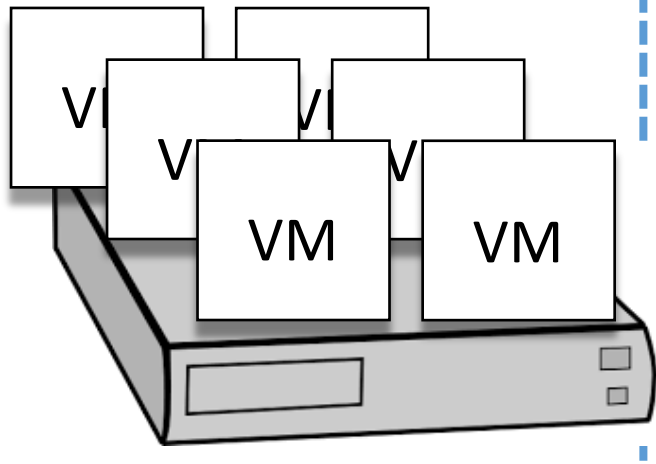


PoPSiCl store

DNS server



SDN controller



Cloud

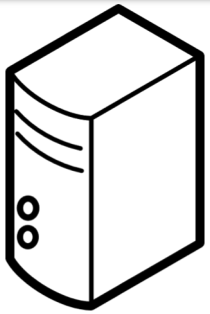
PoPSiCl registration

PoPSiCl

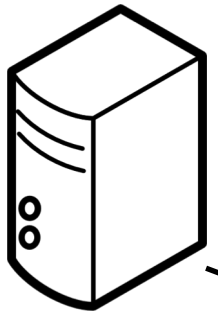
Tenant server ID

PoPSiCl

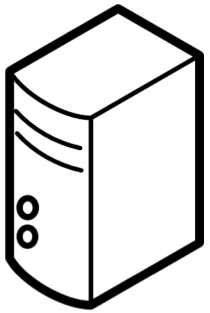
Pseudo IP



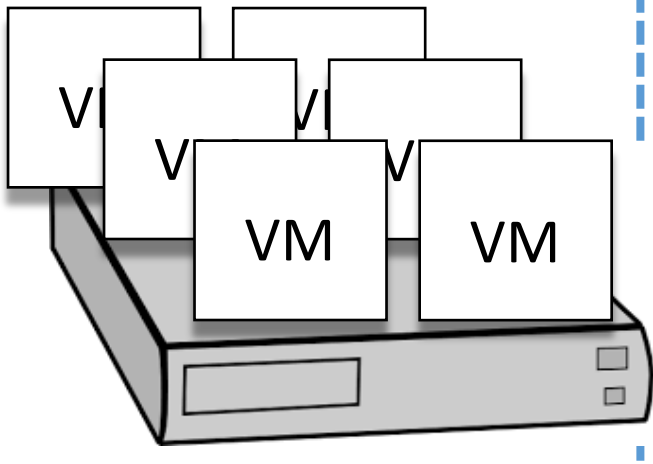
DNS server



PoPSiCl store



SDN controller



Cloud

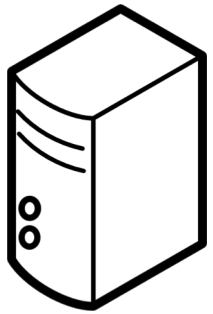
PoPSiCl registration

Client Cert

Server Cert

Client PriKey

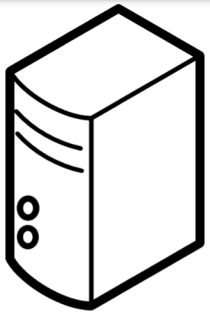
Server PriKey



PoPSiCl store

PoPSiCl

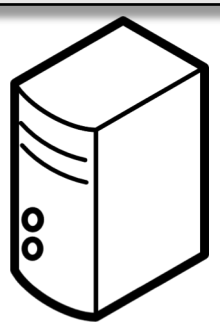
Pseudo IP



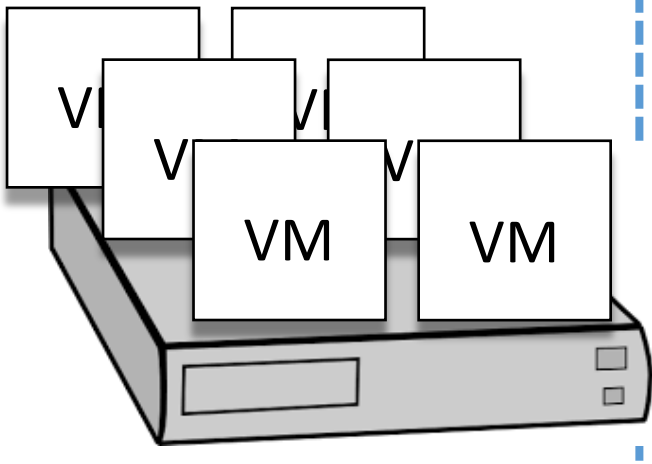
DNS server

PoPSiCl

Tenant server ID



SDN controller



Cloud

PoPSiCl registration

Sign

Cloud PriKey

Client Cert

Server Cert

Client PriKey

Server PriKey

PoPSiCl store

PoPSiCl

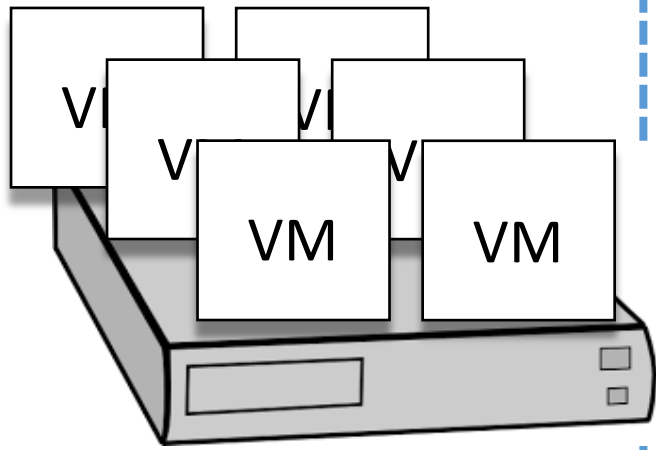
Pseudo IP

DNS server

PoPSiCl

Tenant server ID

SDN controller



Cloud

PoPSiCl registration

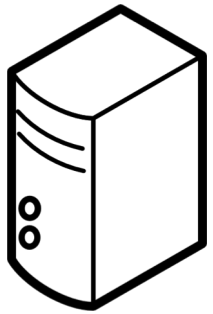
Sign

Server PriKey

Client Cert

Server Cert

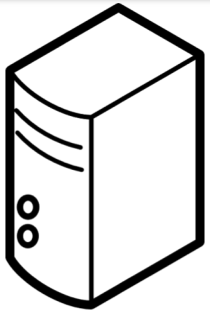
Client PriKey



PoPSiCl store

PoPSiCl

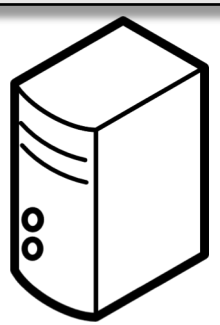
Pseudo IP



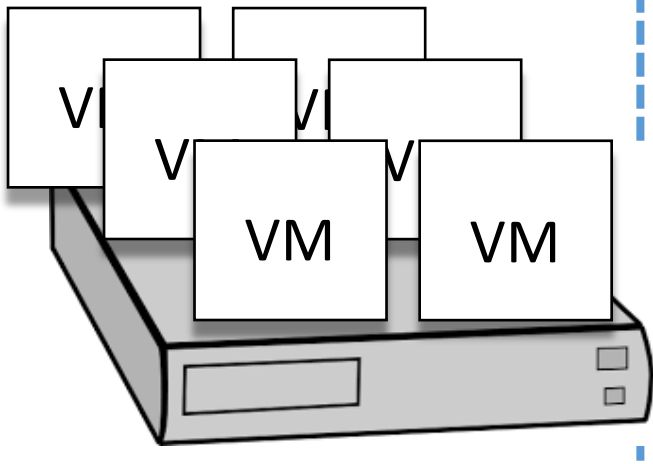
DNS server

PoPSiCl

Tenant server ID



SDN controller



Cloud

PoPSiCl registration

PoPSiCl

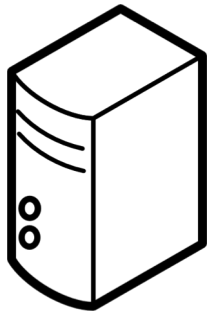
Client Cert

Client PriKey

PoPSiCl

Server Cert

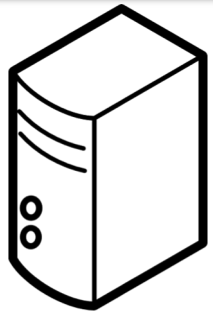
Server PriKey



PoPSiCl store

PoPSiCl

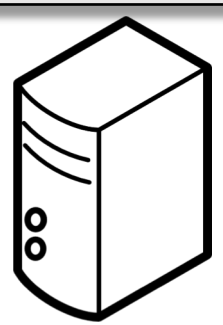
Pseudo IP



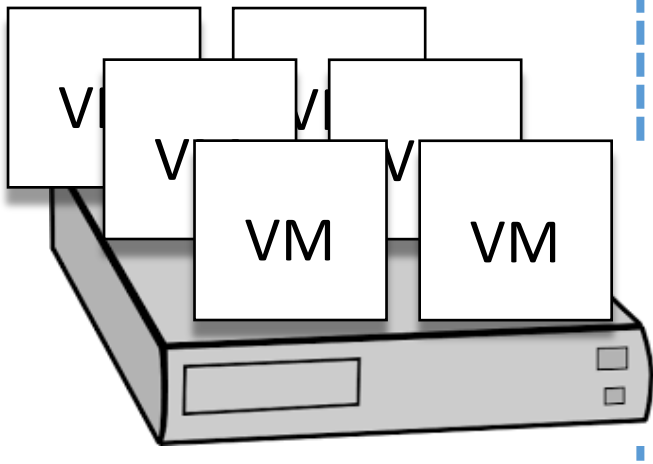
DNS server

PoPSiCl

Tenant server ID



SDN controller



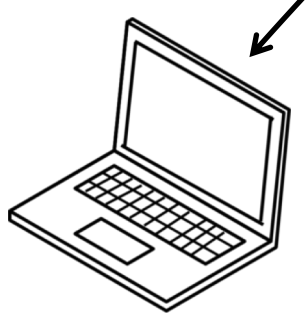
Cloud

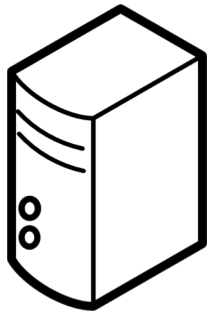
PoPSiCl registration

PoPSiCl

Client Cert

Client PriKey

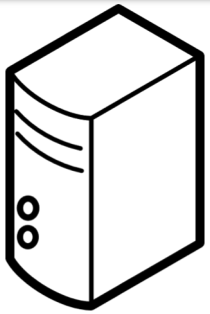




PoPSiCl store

PoPSiCl

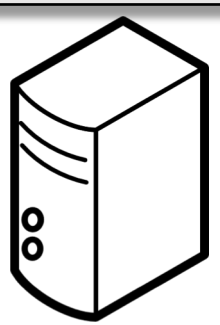
Pseudo IP



DNS server

PoPSiCl

Tenant server ID

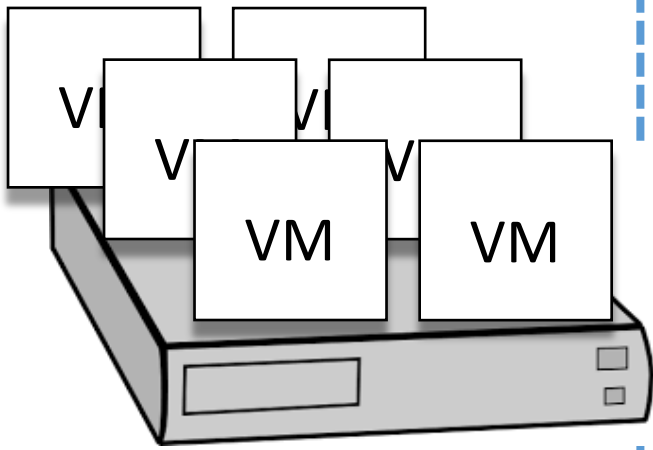


SDN controller

PoPSiCl

Server Cert

Server PriKey



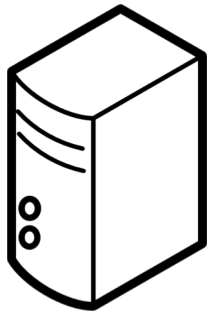
Cloud

PoPSiCl registration

PoPSiCl

Client Cert

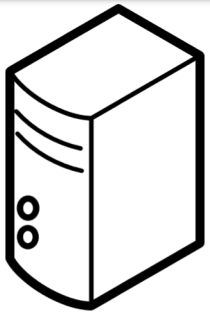
Client PriKey



PoPSiCl store

PoPSiCl

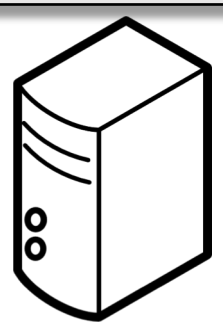
Pseudo IP



DNS server

PoPSiCl

Tenant server ID

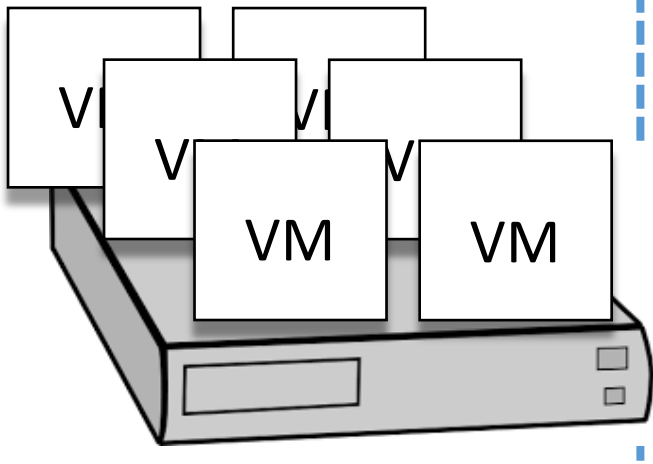


SDN controller

PoPSiCl

Server Cert

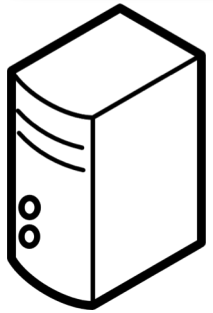
Server PriKey



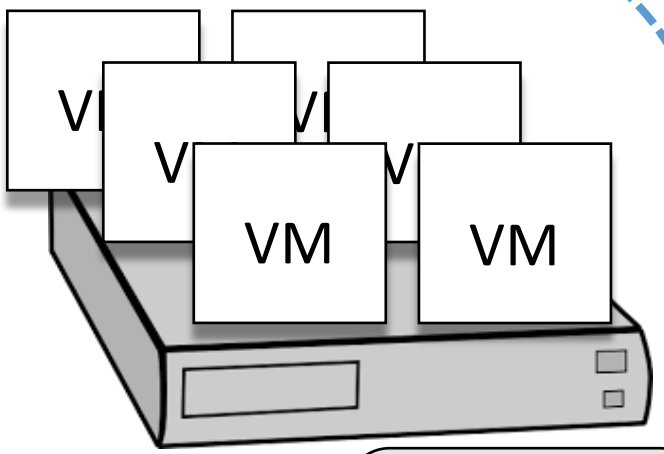
Cloud

PoPSiCl access

PoPSiCl
Pseudo IP

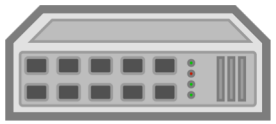


DNS server

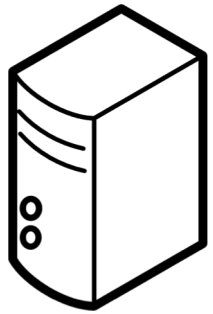


PoPSiCl
Server Cert
Server PriKey

PoPSiCl
Client Cert
Client PriKey



SDN switch

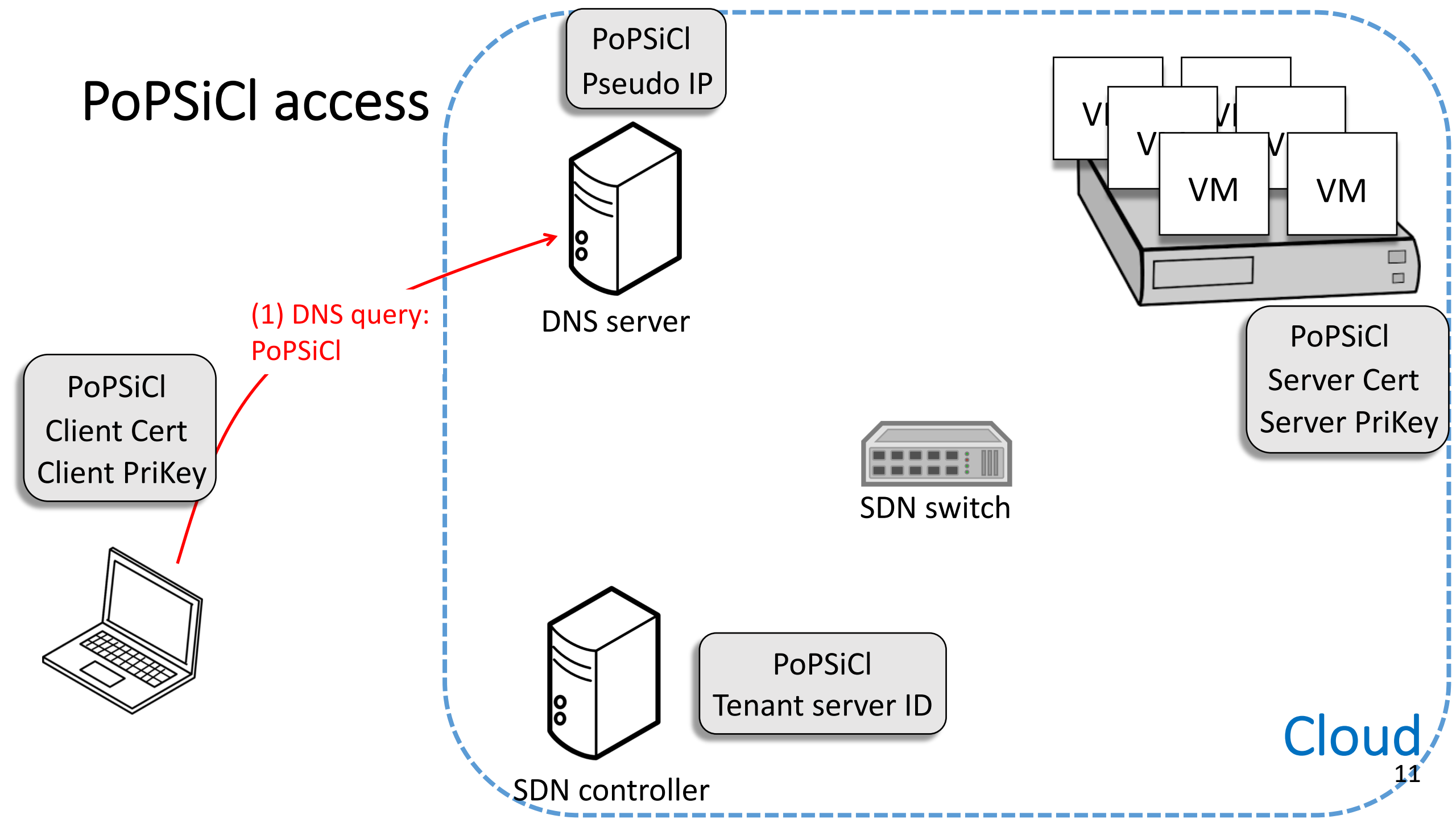


SDN controller

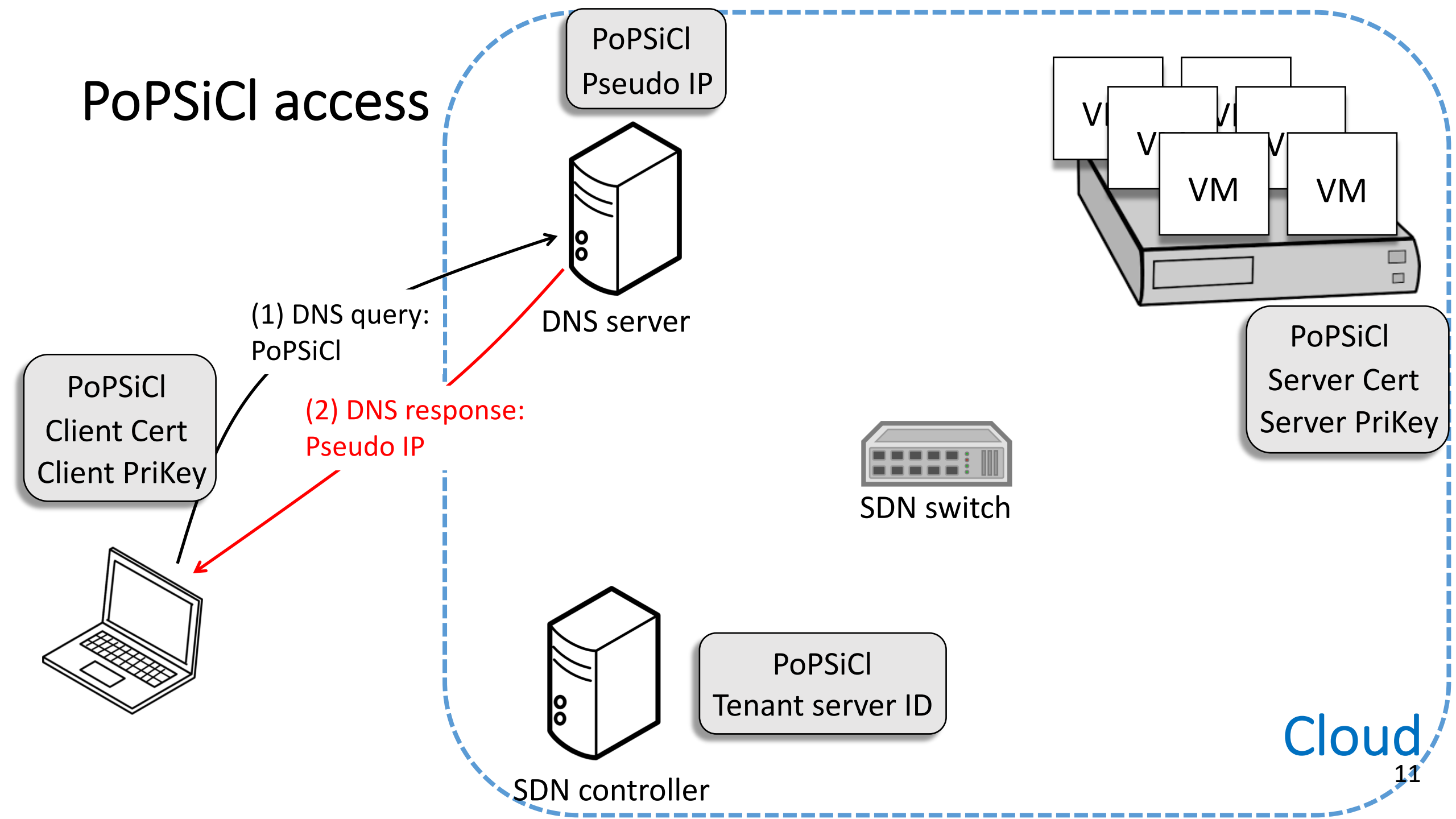
PoPSiCl
Tenant server ID

Cloud

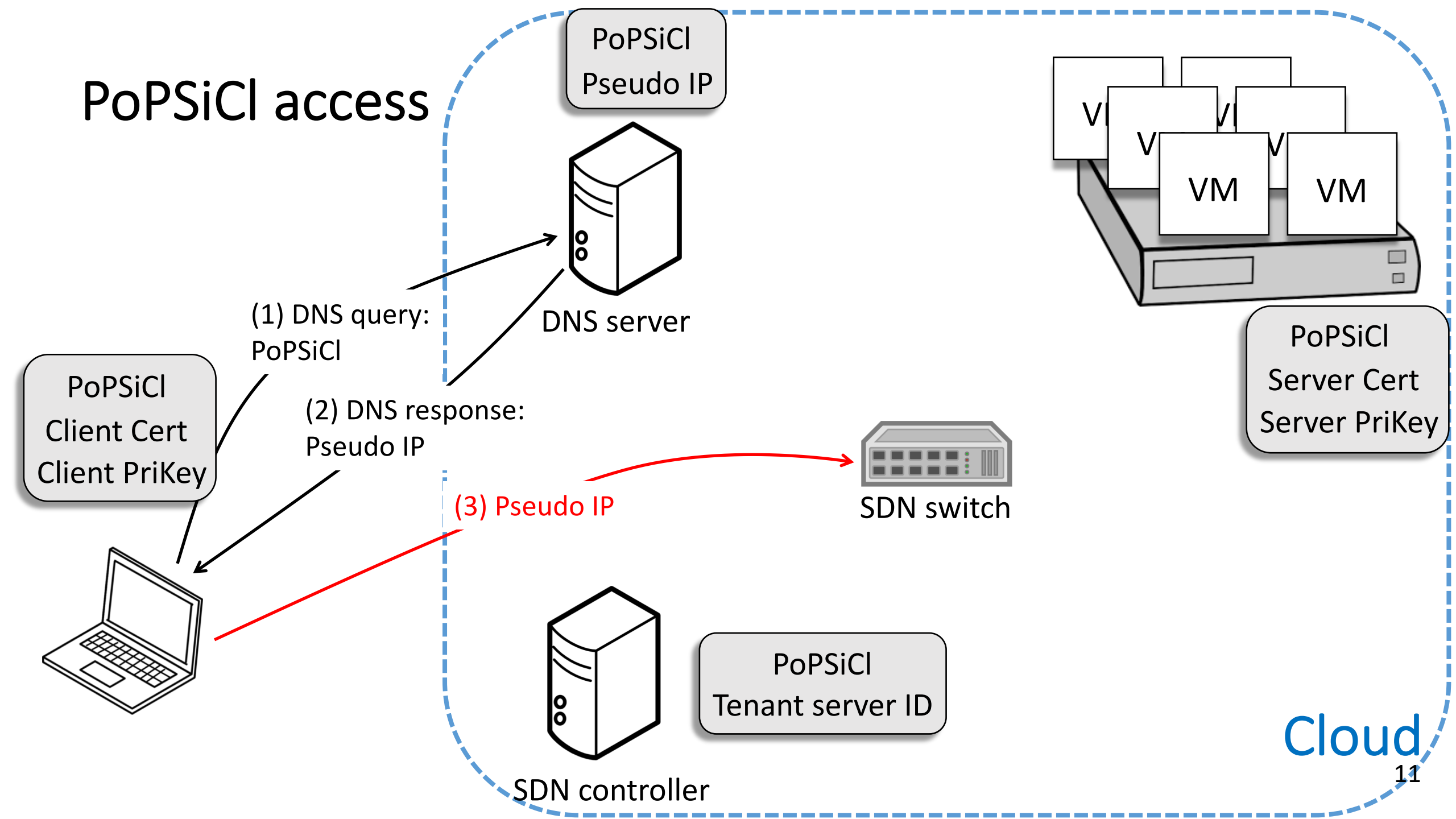
PoPSiCl access



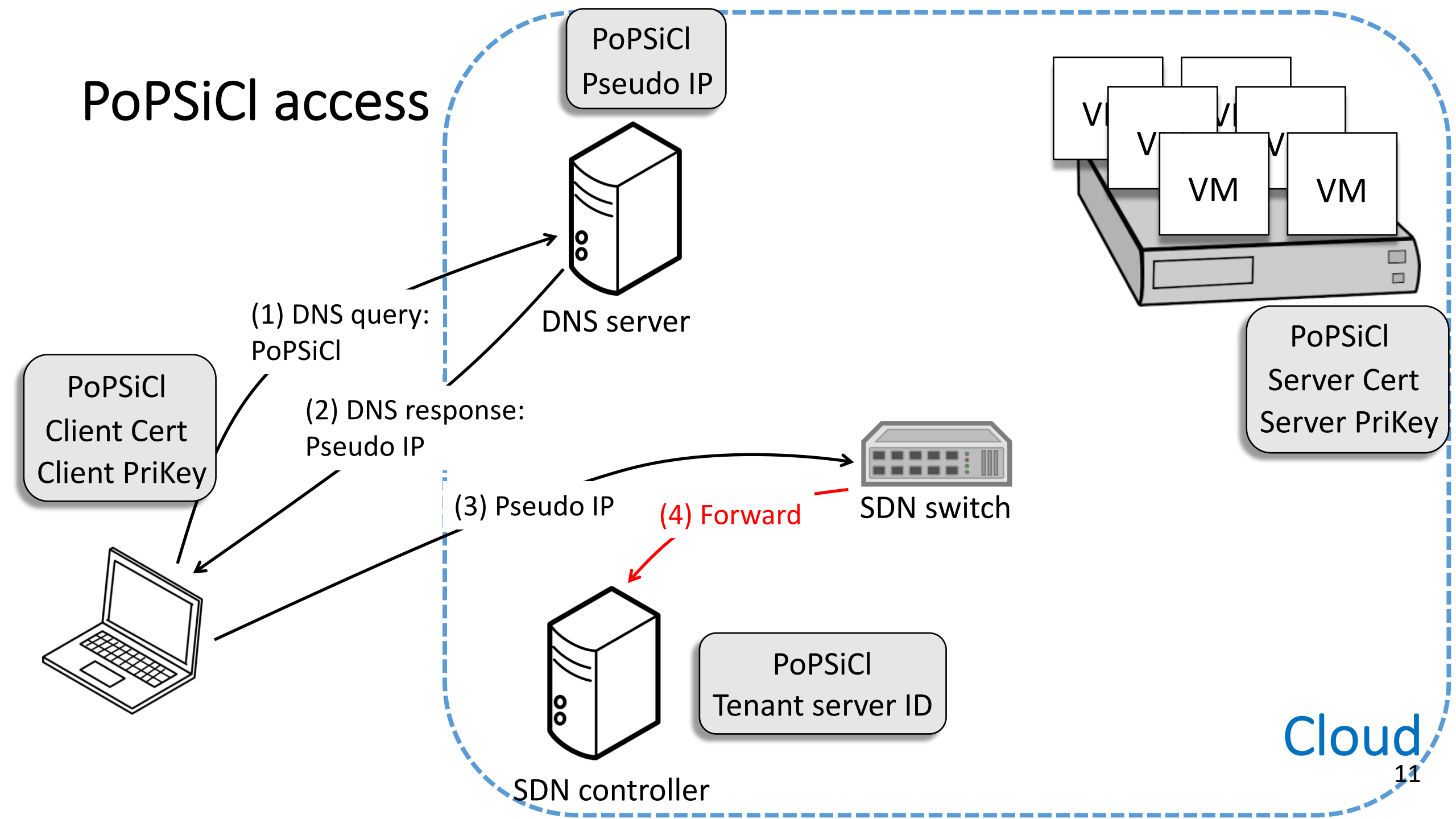
PoPSiCl access



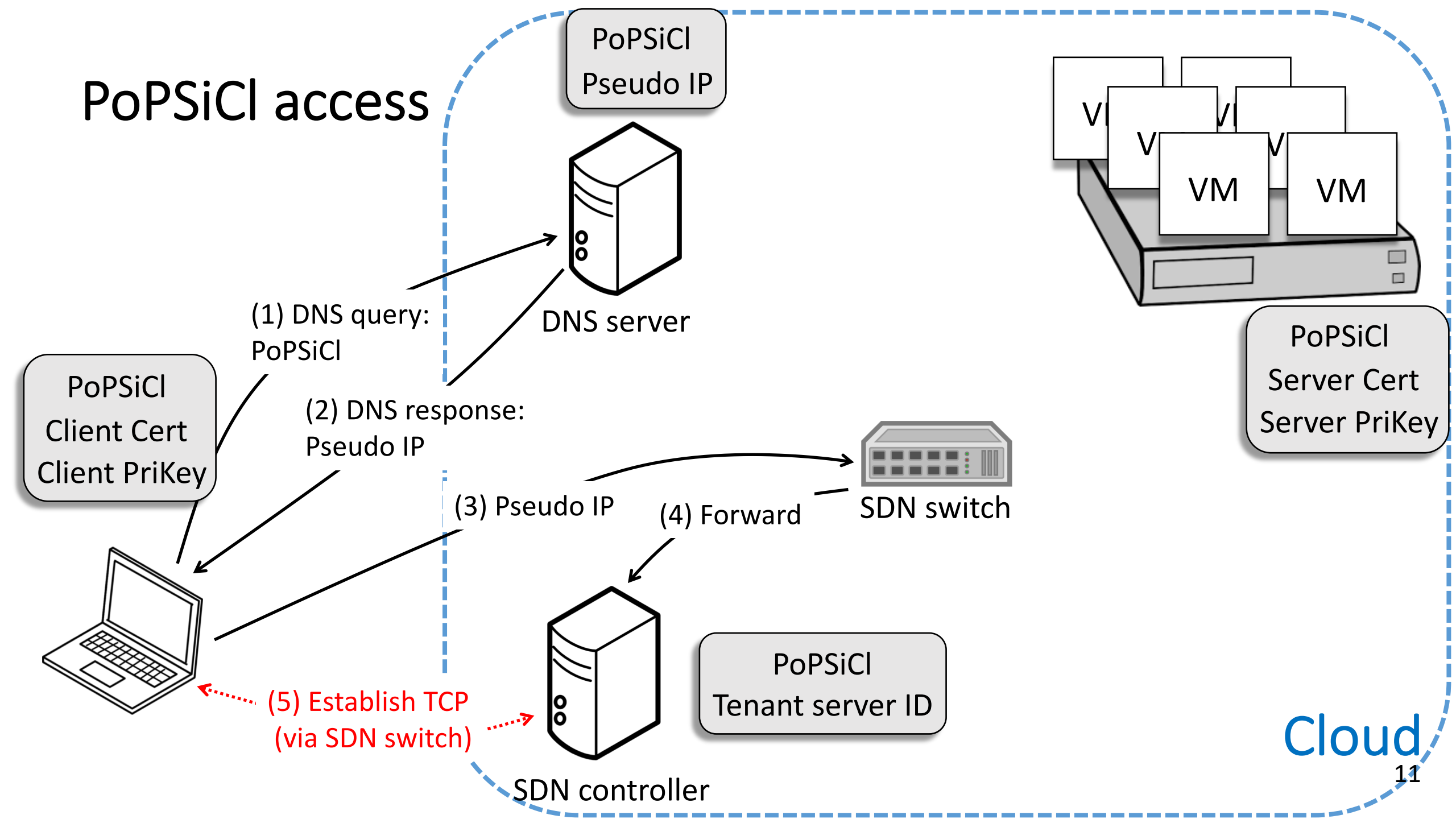
PoPSiCl access



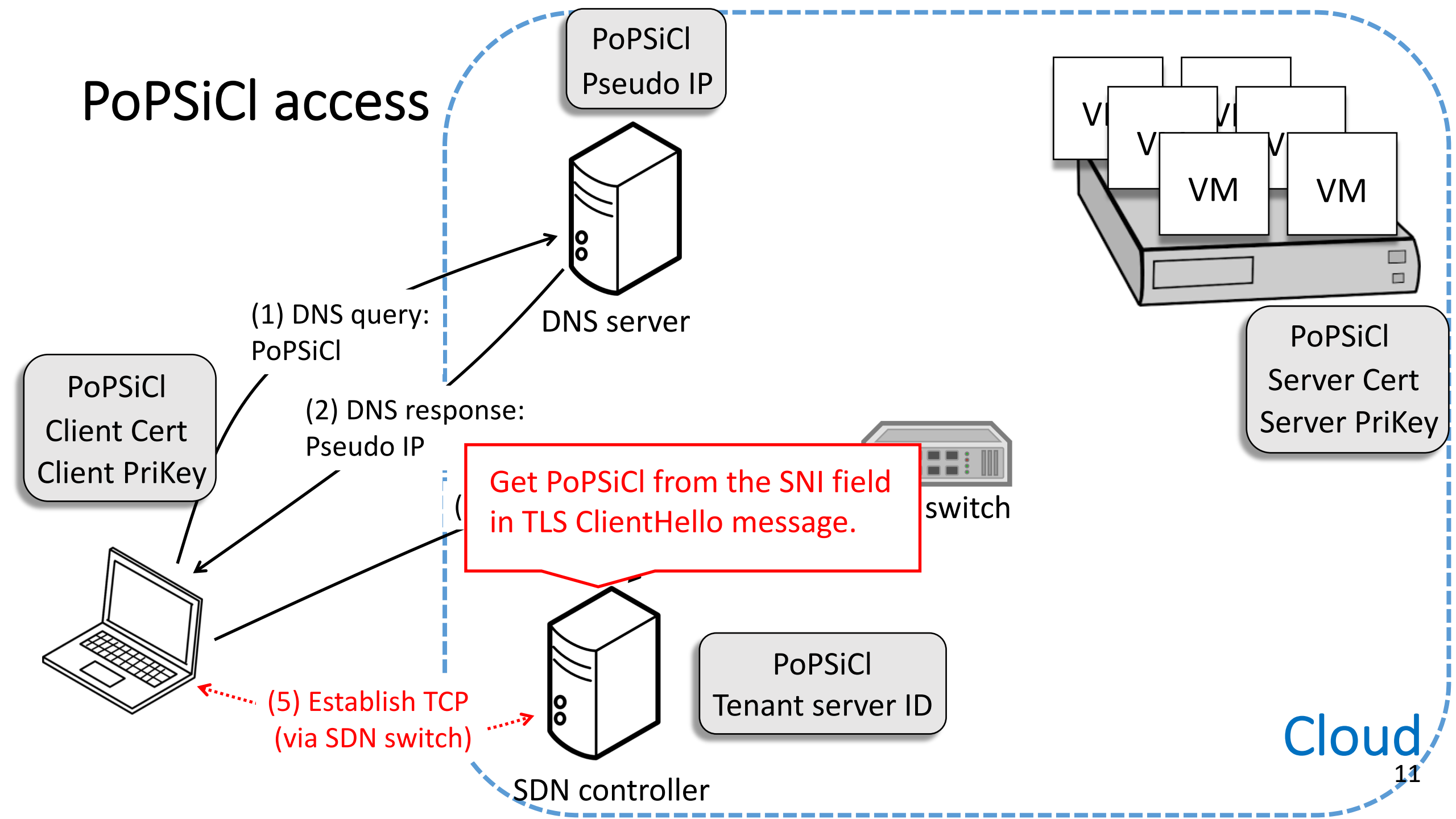
PoPSiCl access



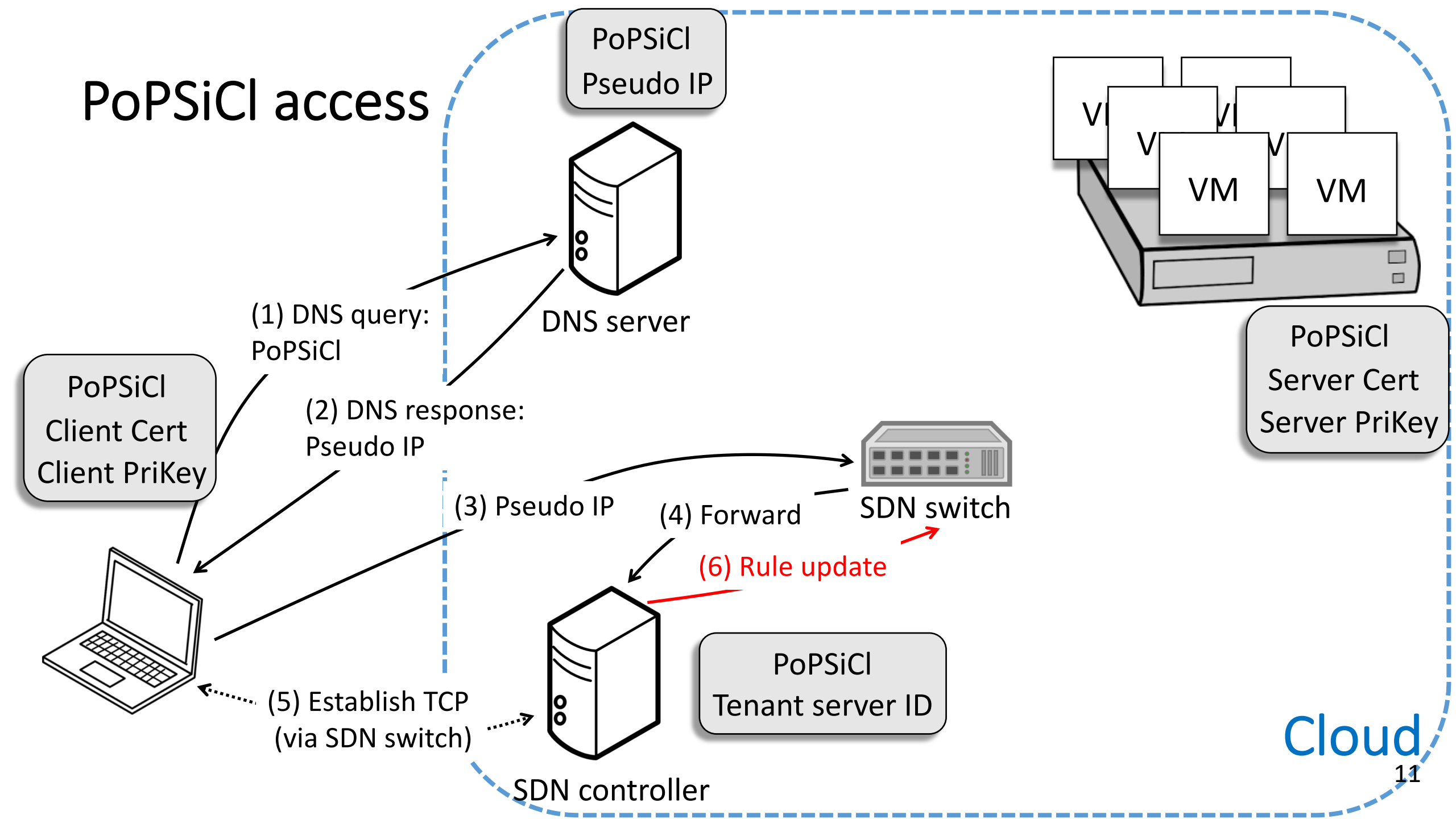
PoPSiCl access



PoPSiCl access



PoPSiCl access



PoPSiCl access

PoPSiCl
Pseudo IP

MATCH				ACTION
Source IP	Source port	Destination IP	Destination port	
Client-IP	*Client-port*	*Pseudo-IP*	*Server-port*	Drop
Tenant-IP	*Server-port*	*Client-IP*	*Client-port*	Change source IP to *Pseudo-IP*

PoPSiCl
Client Cert
Client PriKey

Server Cert
Server PriKey

(2) DNS response:
Pseudo IP

(3) Pseudo IP

(4) Forward

SDN switch

(6) Rule update

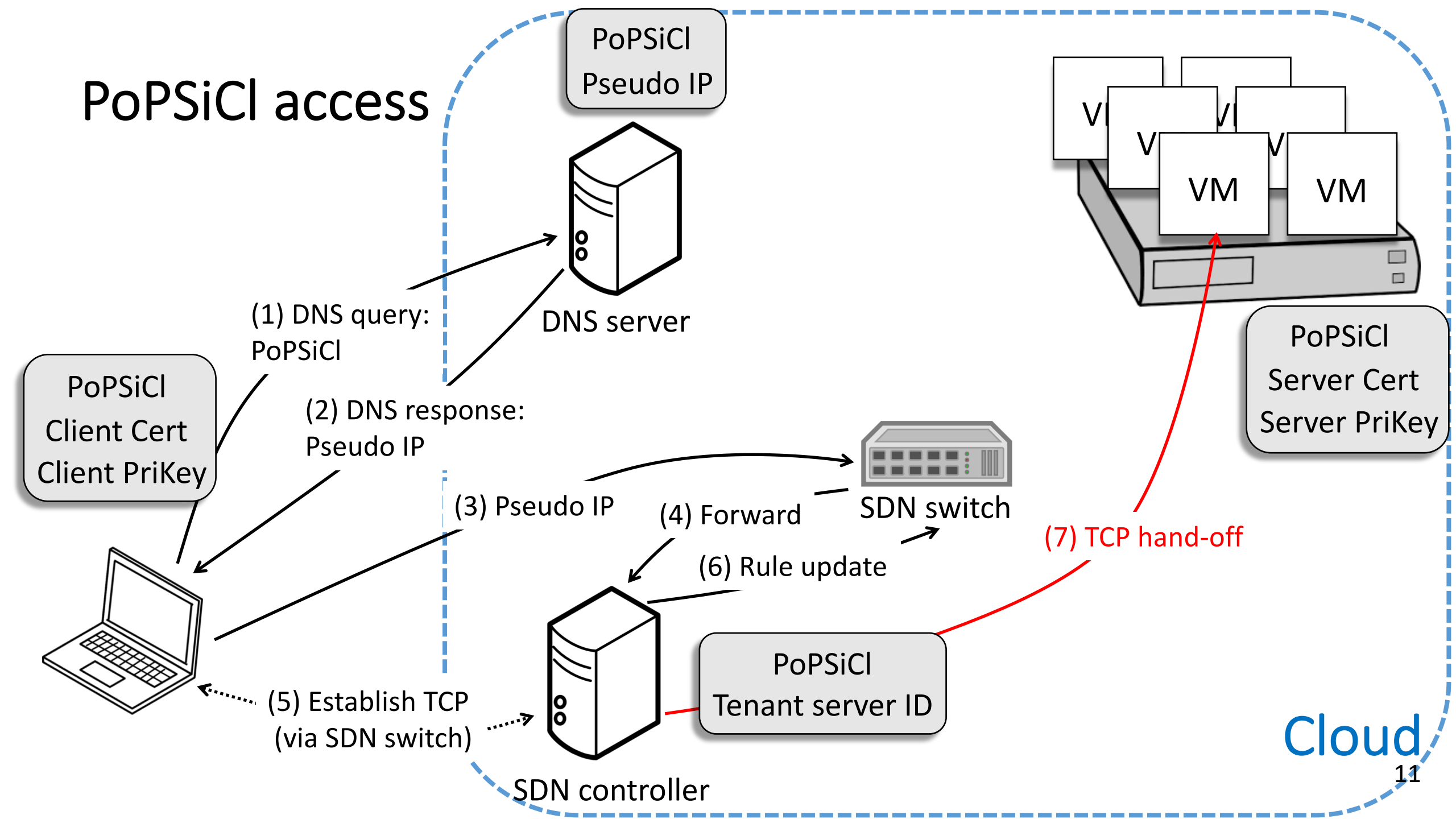
(5) Establish TCP
(via SDN switch)

PoPSiCl
Tenant server ID

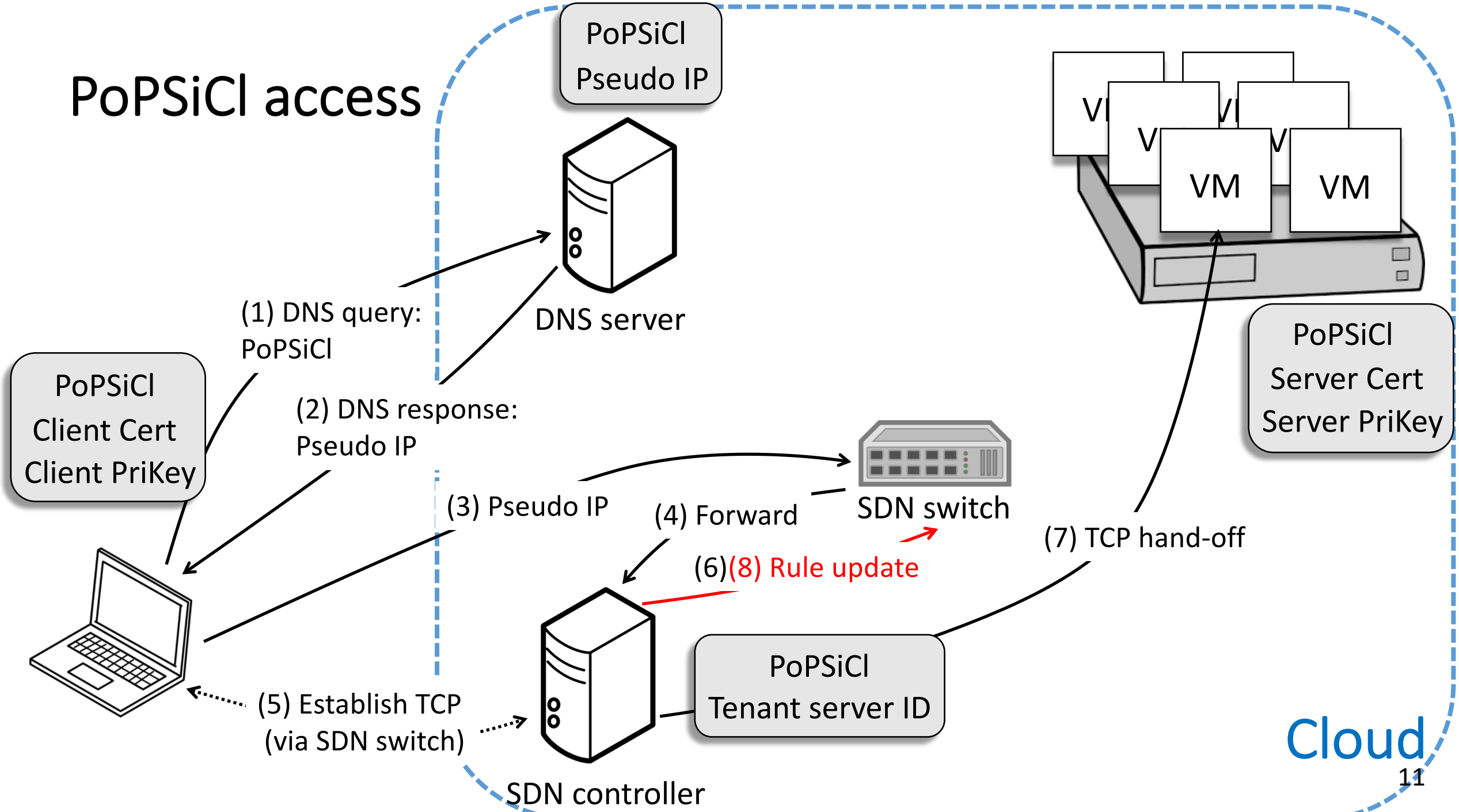
SDN controller

Cloud

PoPSiCl access



PoPSiCl access



PoPSiCl access

PoPSiCl
Pseudo IP

MATCH				ACTION
Source IP	Source port	Destination IP	Destination port	
Client-IP	*Client-port*	*Pseudo-IP*	*Server-port*	Change destination IP to *Tenant-IP*
Tenant-IP	*Server-port*	*Client-IP*	*Client-port*	Change source IP to *Pseudo-IP*

PoPSiCl
Client Cert
Client PriKey

PoPSiCl
Server Cert
Server PriKey

(2) DNS response:
Pseudo IP

(3) Pseudo IP

(4) Forward

SDN switch

(6)(8) Rule update

(7) TCP hand-off

(5) Establish TCP
(via SDN switch)

PoPSiCl
Tenant server ID

SDN controller

Cloud

PoPSiCl access

PoPSiCl
Pseudo IP

MATCH				ACTION
Source IP	Source port	Destination IP	Destination port	
Client-IP	*Client-port*	*Pseudo-IP*	*Server-port*	Change destination IP to *Tenant-IP*
Tenant-IP	*Server-port*	*Client-IP*	*Client-port*	Change source IP to *Pseudo-IP*

PoPSiCl
Client Cert
Client PriKey

PoPSiCl
Server Cert
Server PriKey

(2) DNS response:
Pseudo IP

(3) Pseudo IP

(4) Forward

SDN switch

(6)(8) Rule update

(7) TCP hand-off

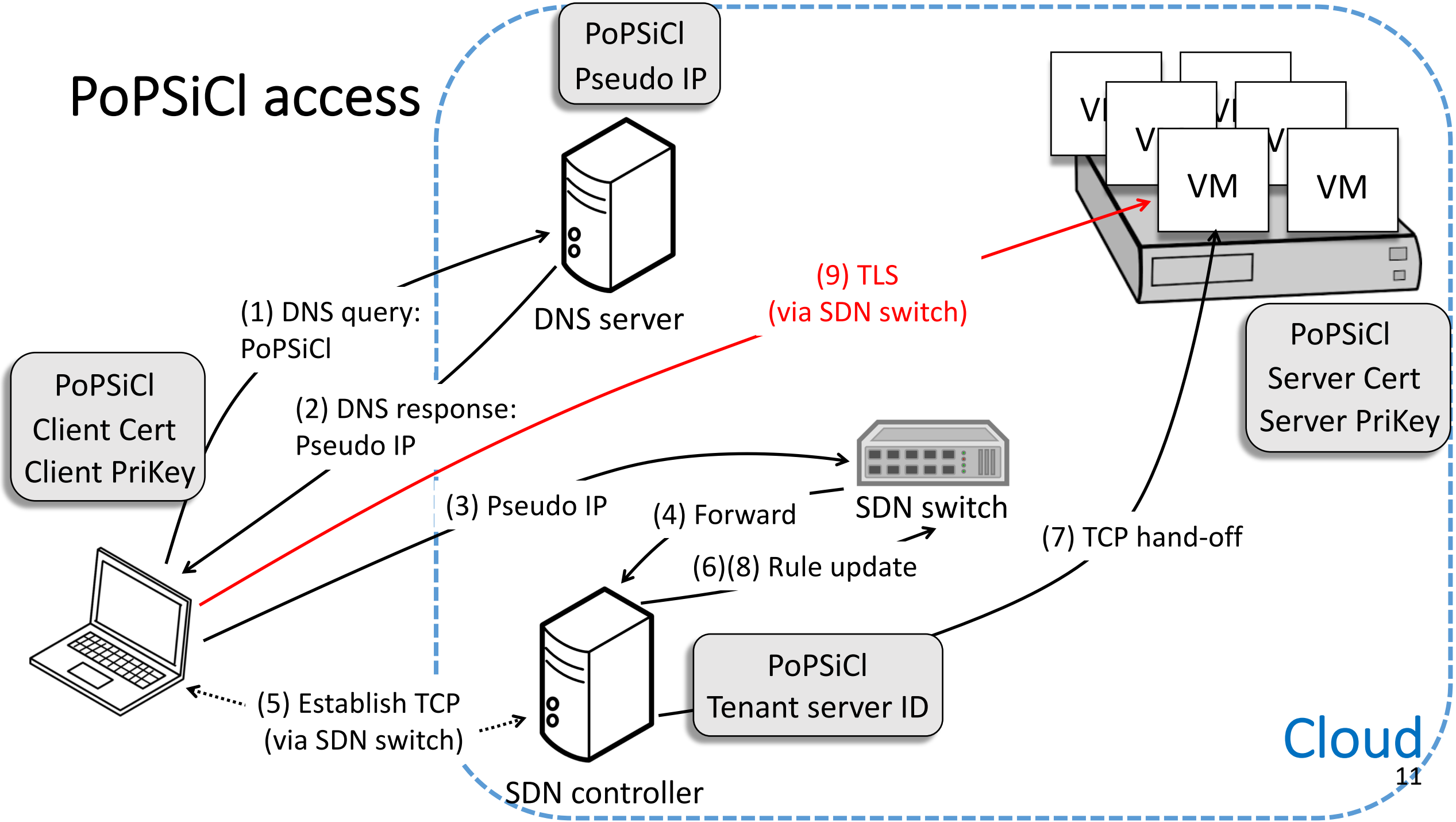
(5) Establish TCP
(via SDN switch)

PoPSiCl
Tenant server ID

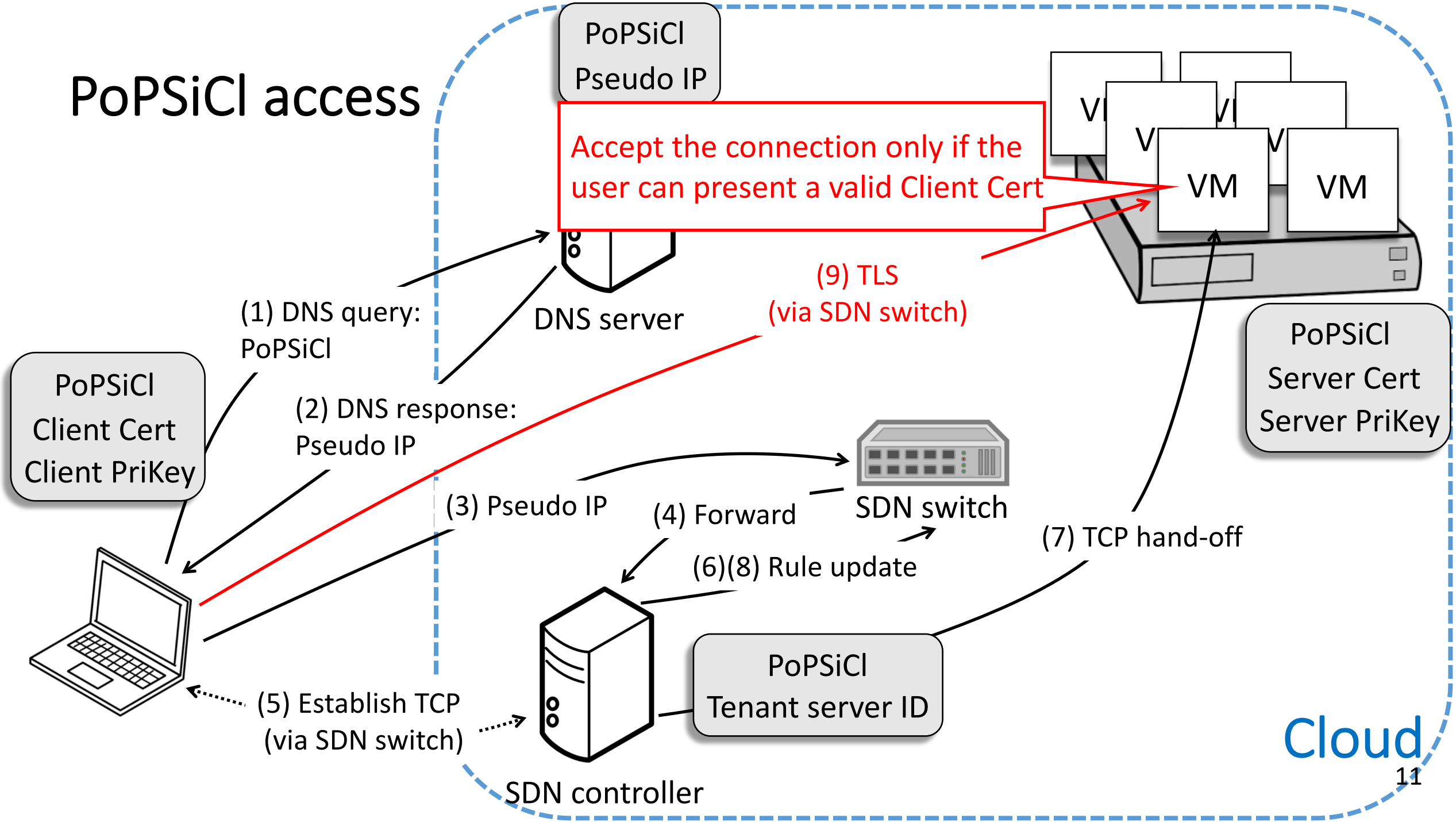
SDN controller

Cloud

PoPSiCl access



PoPSiCl access



Implementation

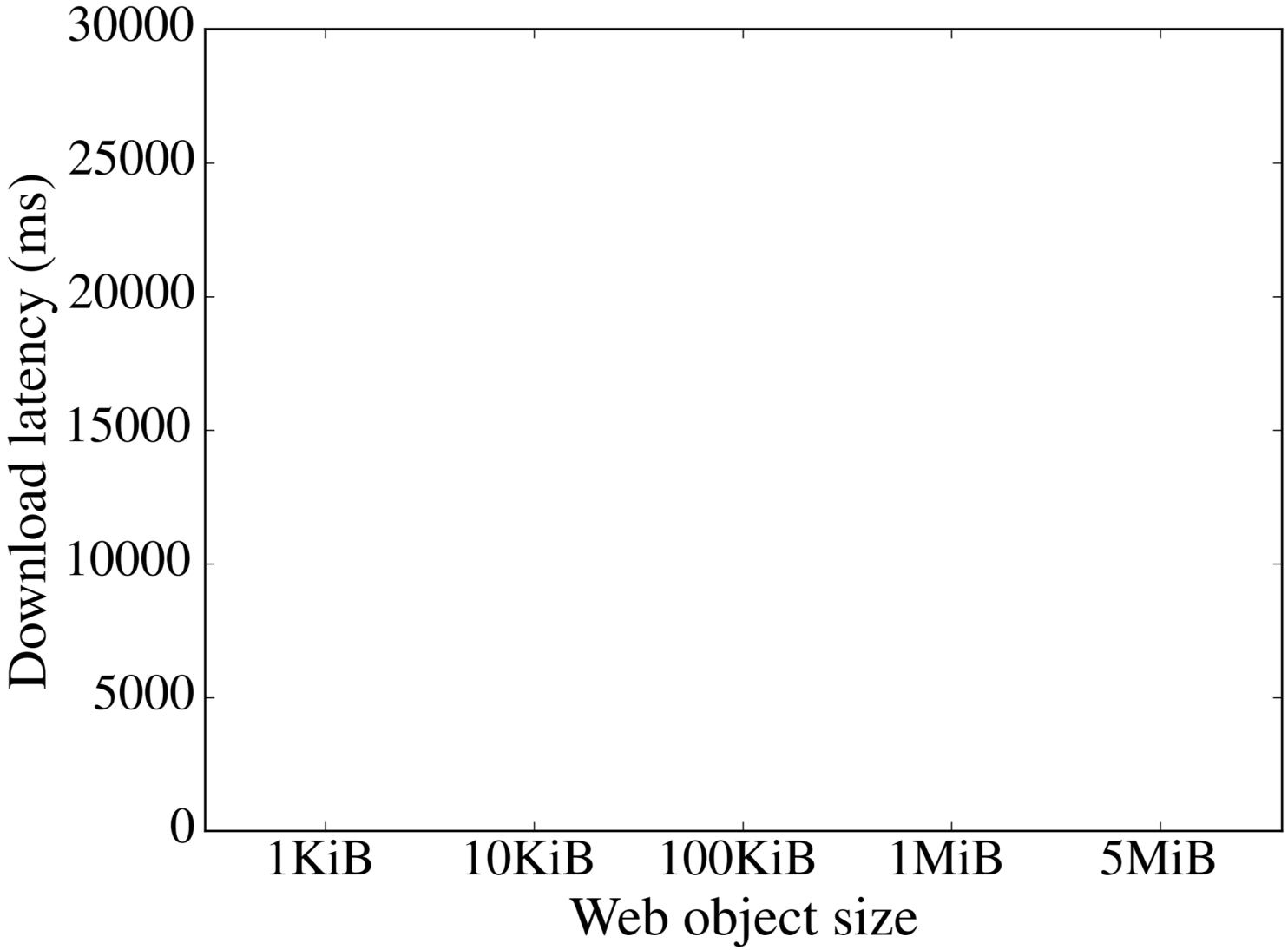
Cloud

- OpenStack-based IaaS cloud deployed in CloudLab testbed
- PoPSiCl store and SDN controller are implemented in C and C++
- Open vSwitch as the SDN switch in each physical machine

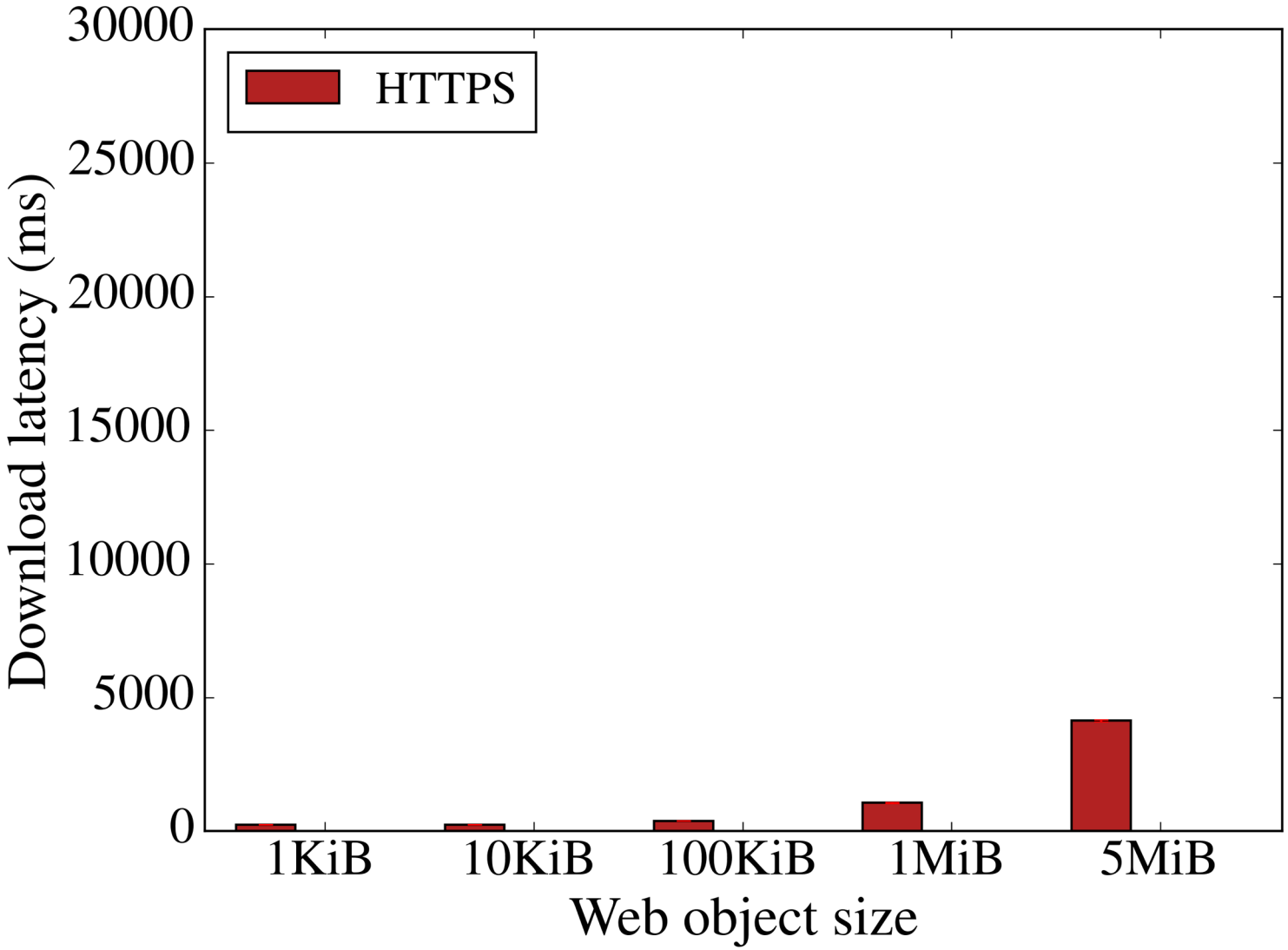
Tenant server

- A Linux kernel module for TCP state transfer
- Each PoPSiCl is mapped to a virtual host in Nginx server

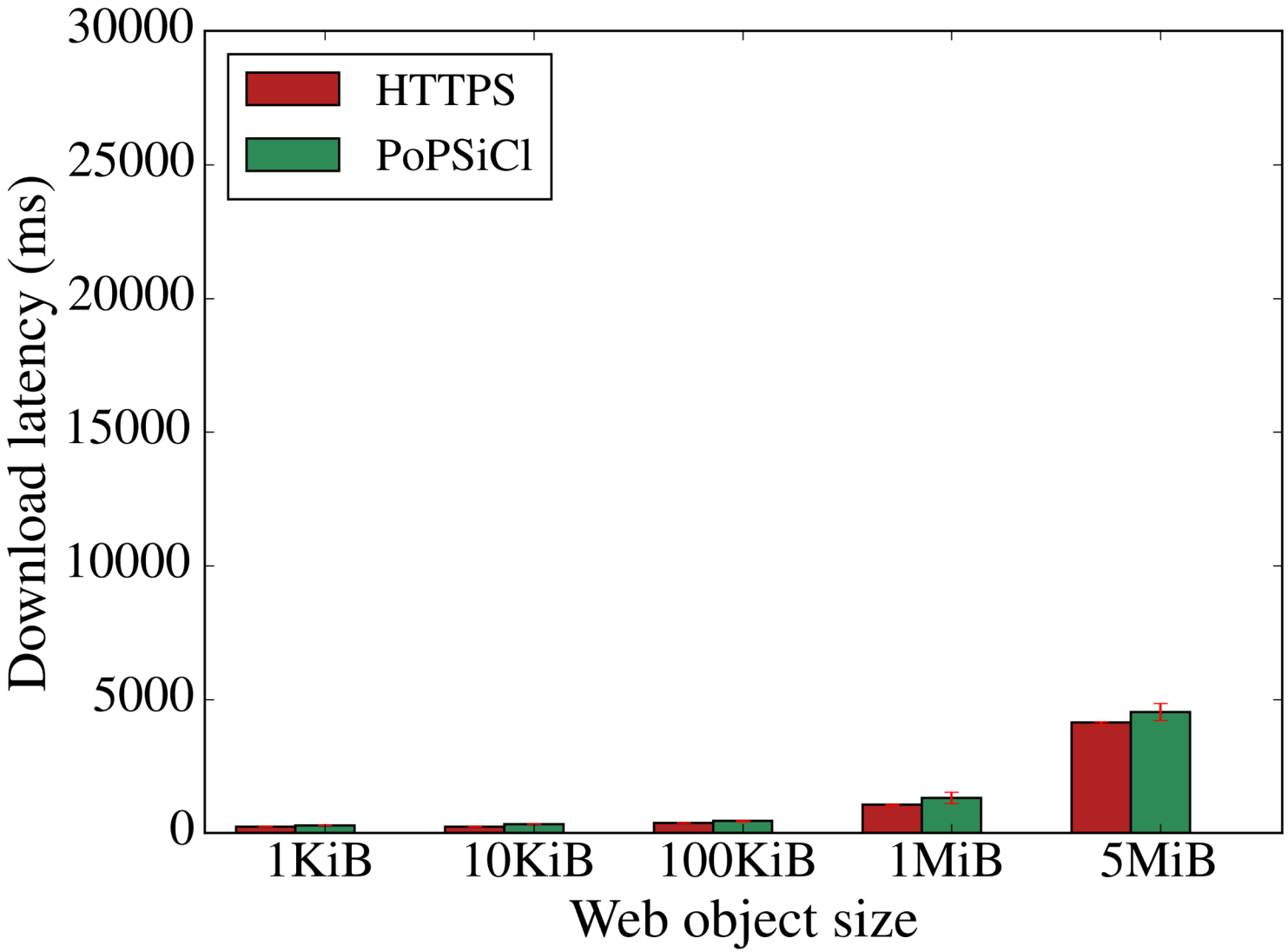
Latency


30000
25000
20000
15000
10000
5000
0
Download latency (ms)
1KiB
10KiB
100KiB
1MiB
5MiB
Web object size

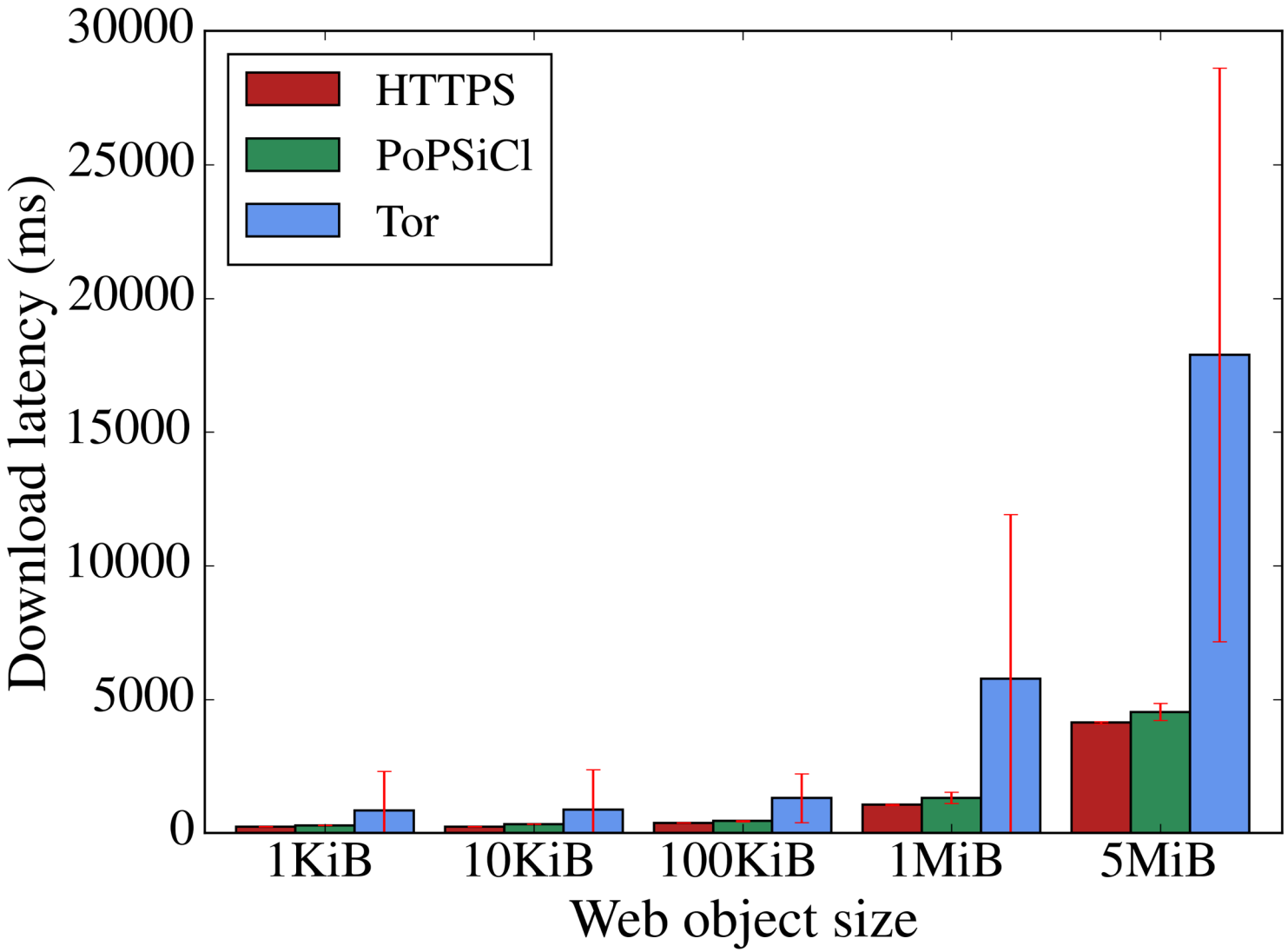
Latency


HTTPS
30000
25000
20000
15000
10000
5000
0
Download latency (ms)
1KiB
10KiB
100KiB
1MiB
5MiB
Web object size

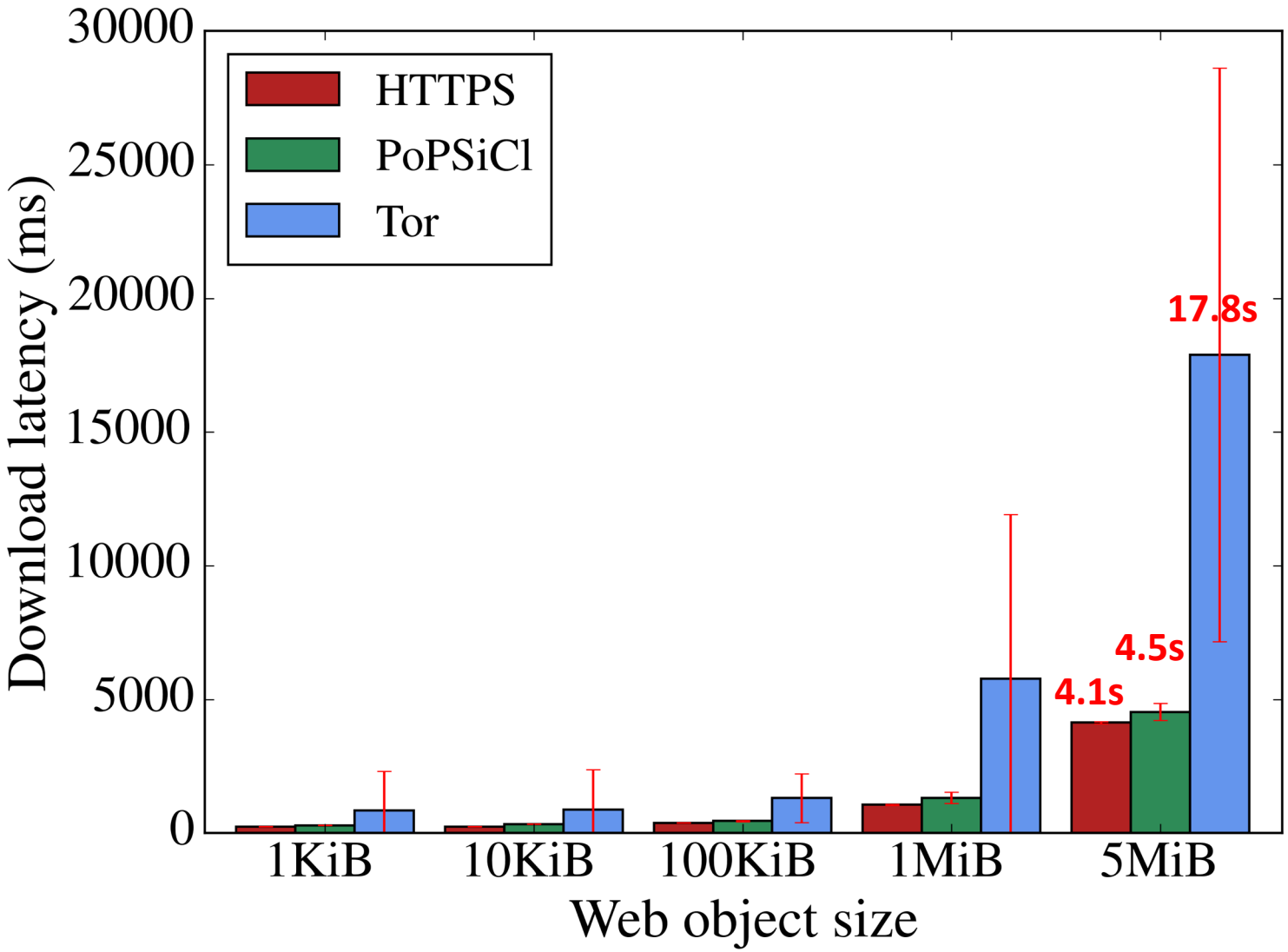
Latency


30000
25000
20000
15000
10000
5000
0
Download latency (ms)
HTTPS
PoPSiCl
1KiB
10KiB
100KiB
1MiB
5MiB
Web object size

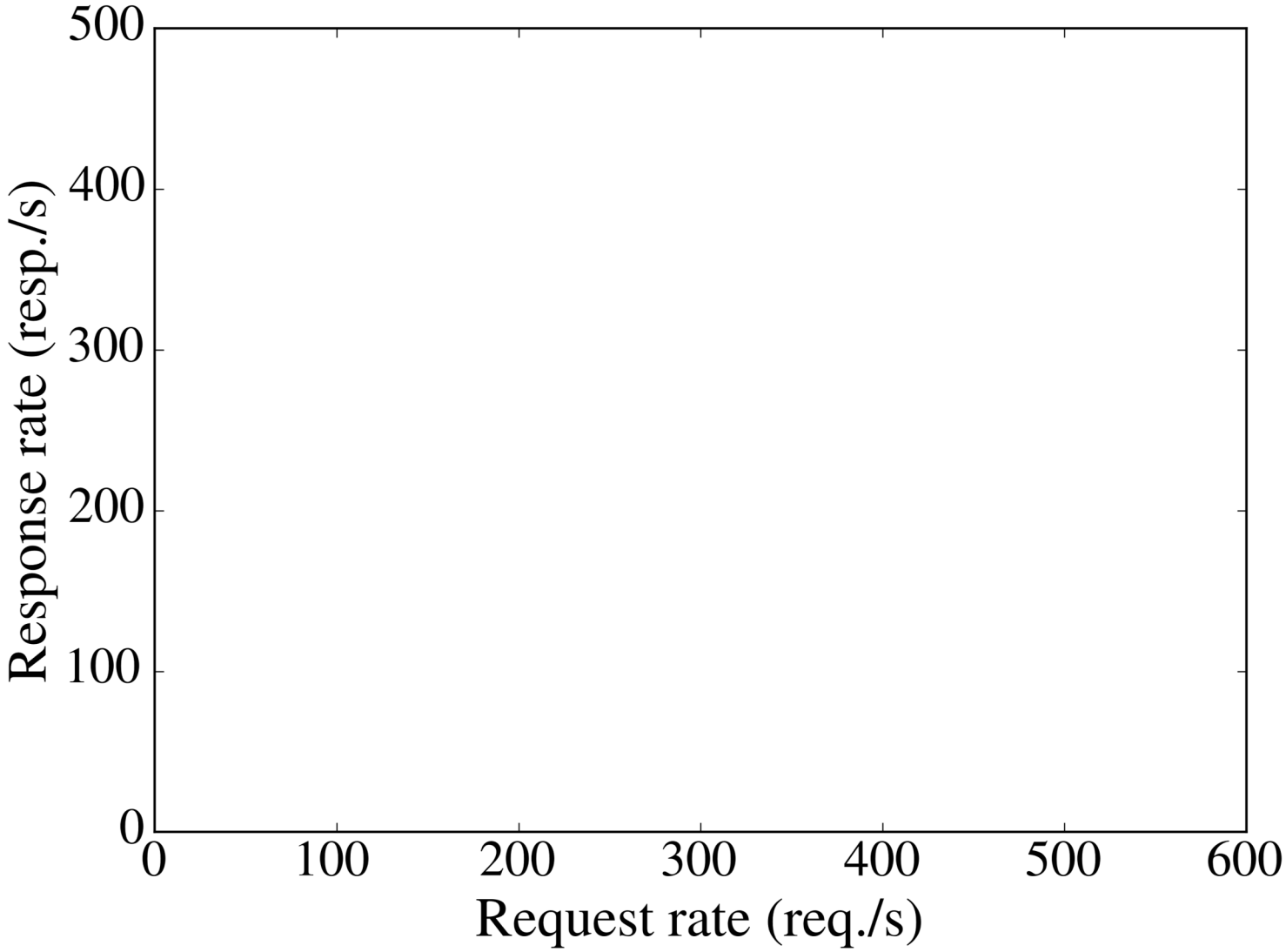
Latency


30000
25000
20000
15000
10000
5000
0
Download latency (ms)
HTTPS
PoPSiCl
Tor
1KiB
10KiB
100KiB
1MiB
5MiB
Web object size

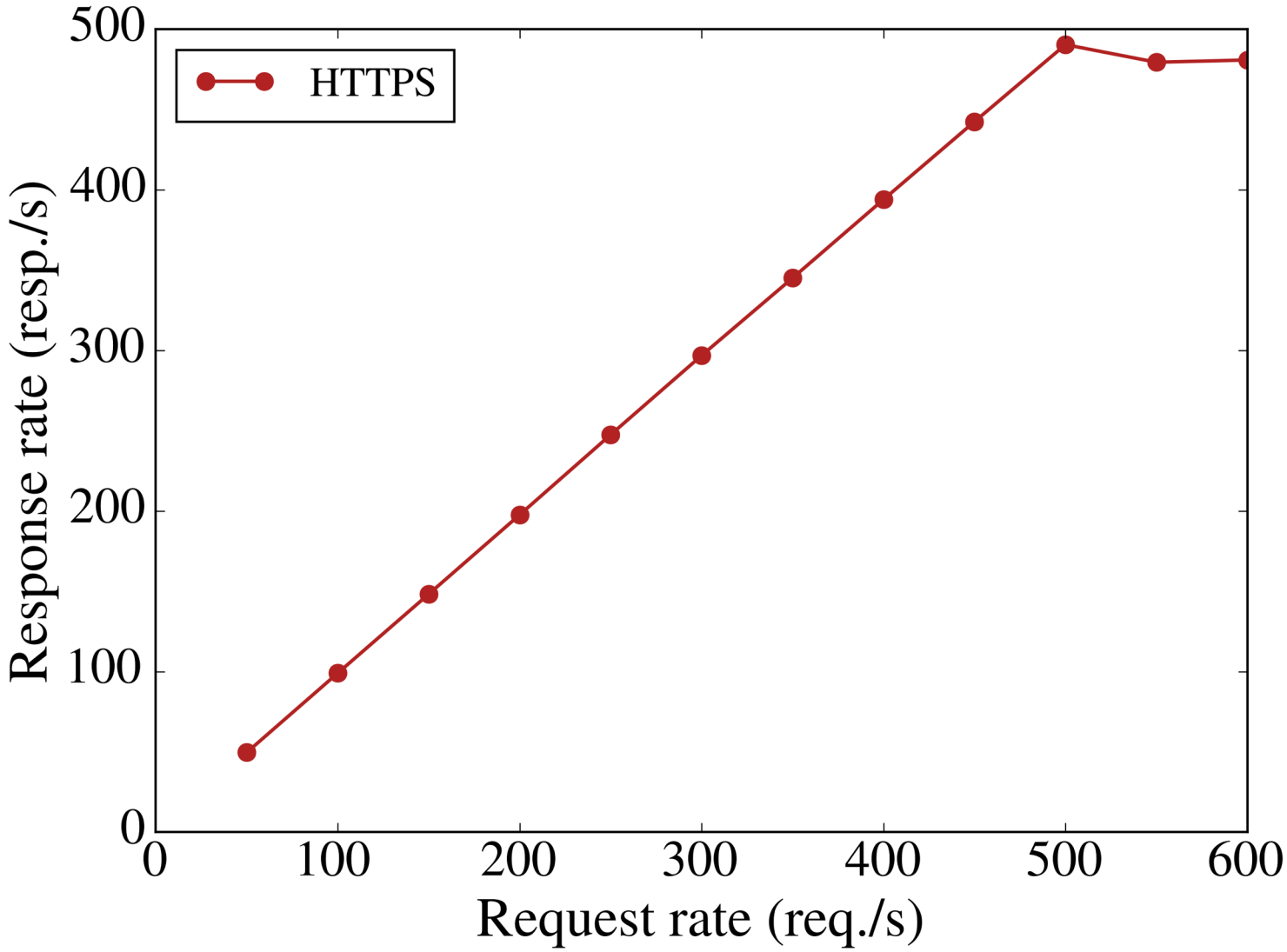
Latency


30000
25000
20000
15000
10000
5000
0
Download latency (ms)
HTTPS
PoPSiCl
Tor
17.8s
4.5s
4.1s
1KiB
10KiB
100KiB
1MiB
5MiB
Web object size

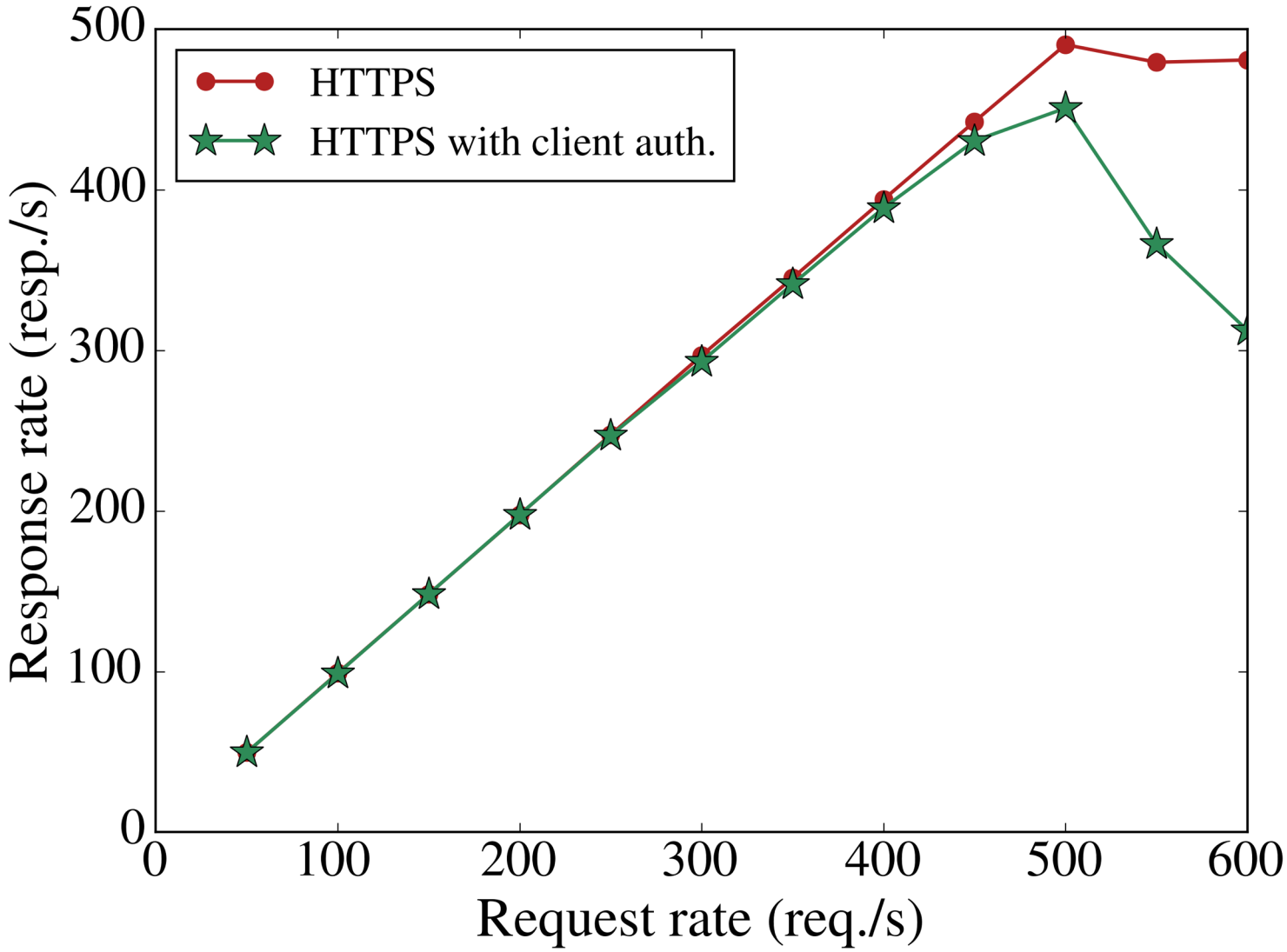
Throughput


500
400
300
200
100
0
Response rate (resp./s)
0
100
200
300
400
500
600
Request rate (req./s)

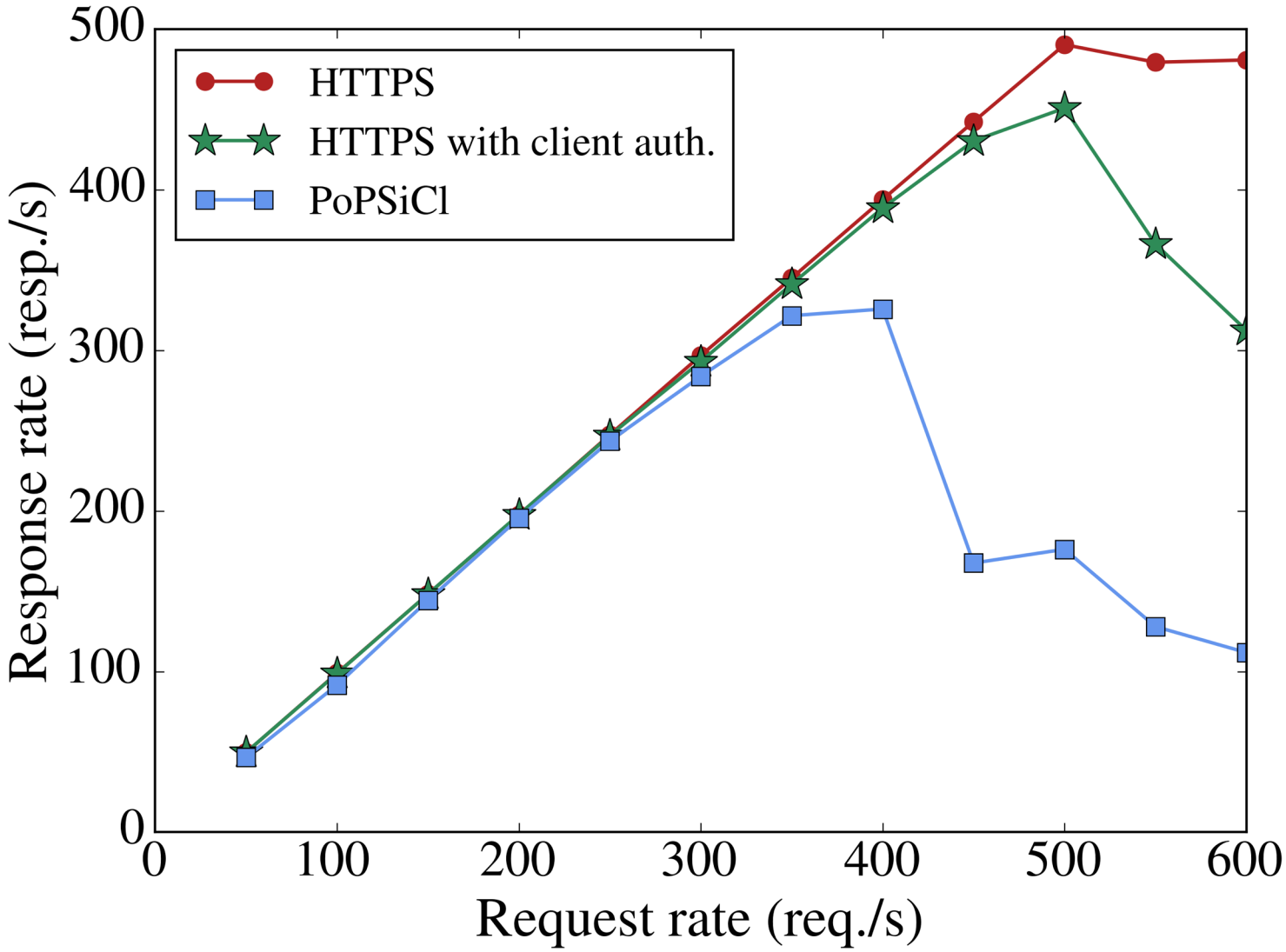
Throughput


HTTPS
Response rate (resp./s)
Request rate (req./s)
0
100
200
300
400
500
600

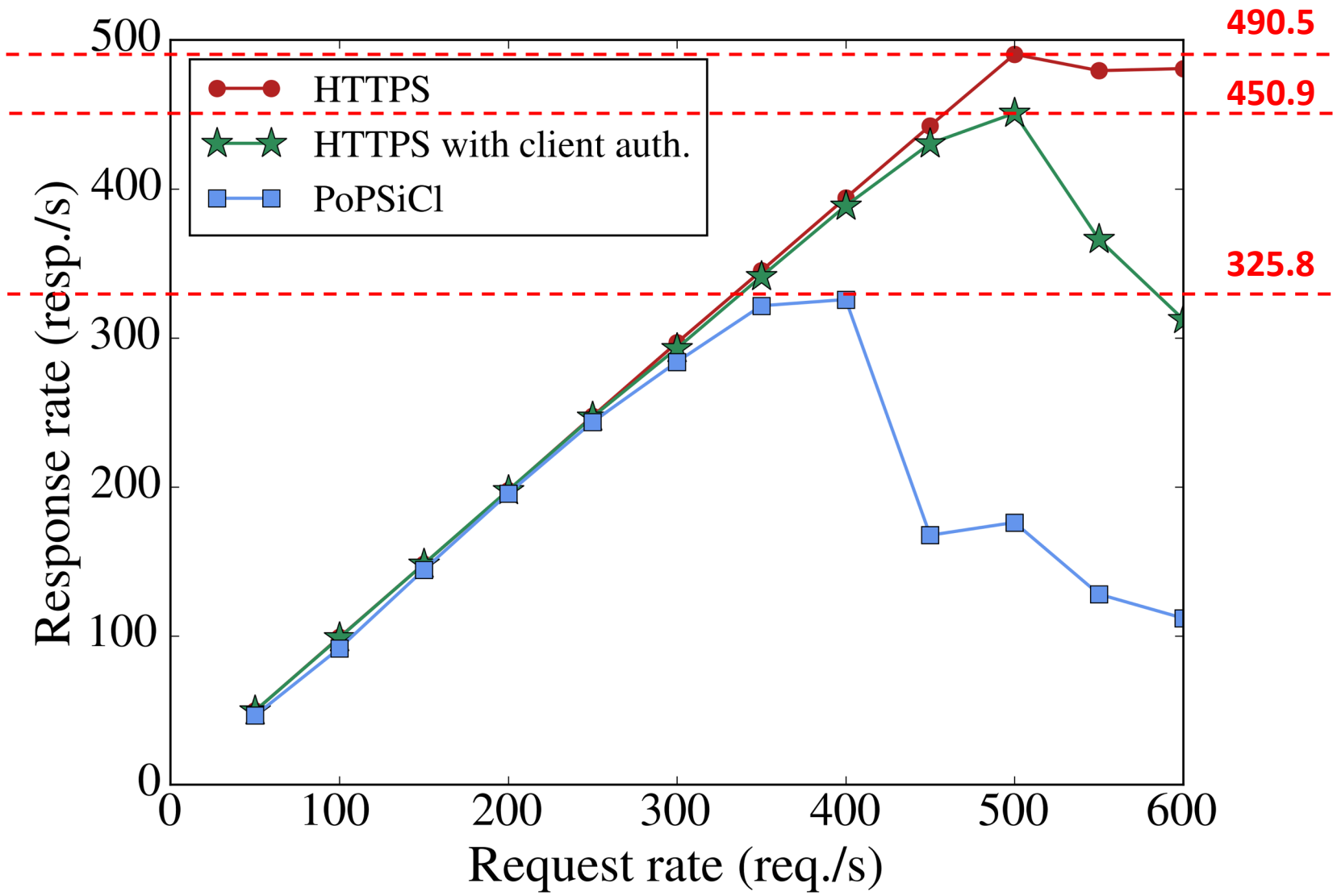
Throughput


HTTPS
HTTPS with client auth.
Response rate (resp./s)
Request rate (req./s)
0
100
200
300
400
500
600

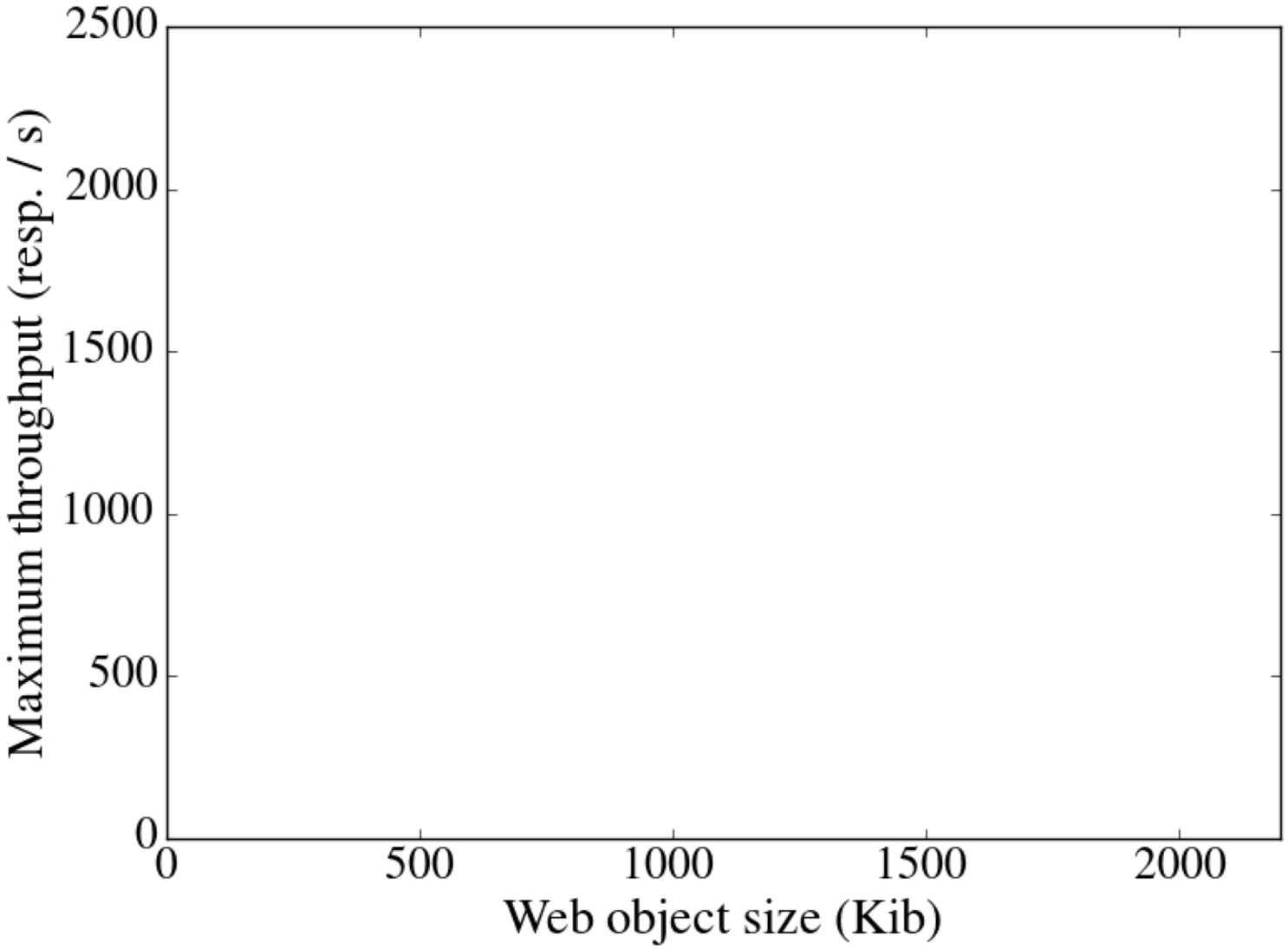
Throughput


HTTPS
HTTPS with client auth.
PoPSiCl
Response rate (resp./s)
Request rate (req./s)
0
100
200
300
400
500
600

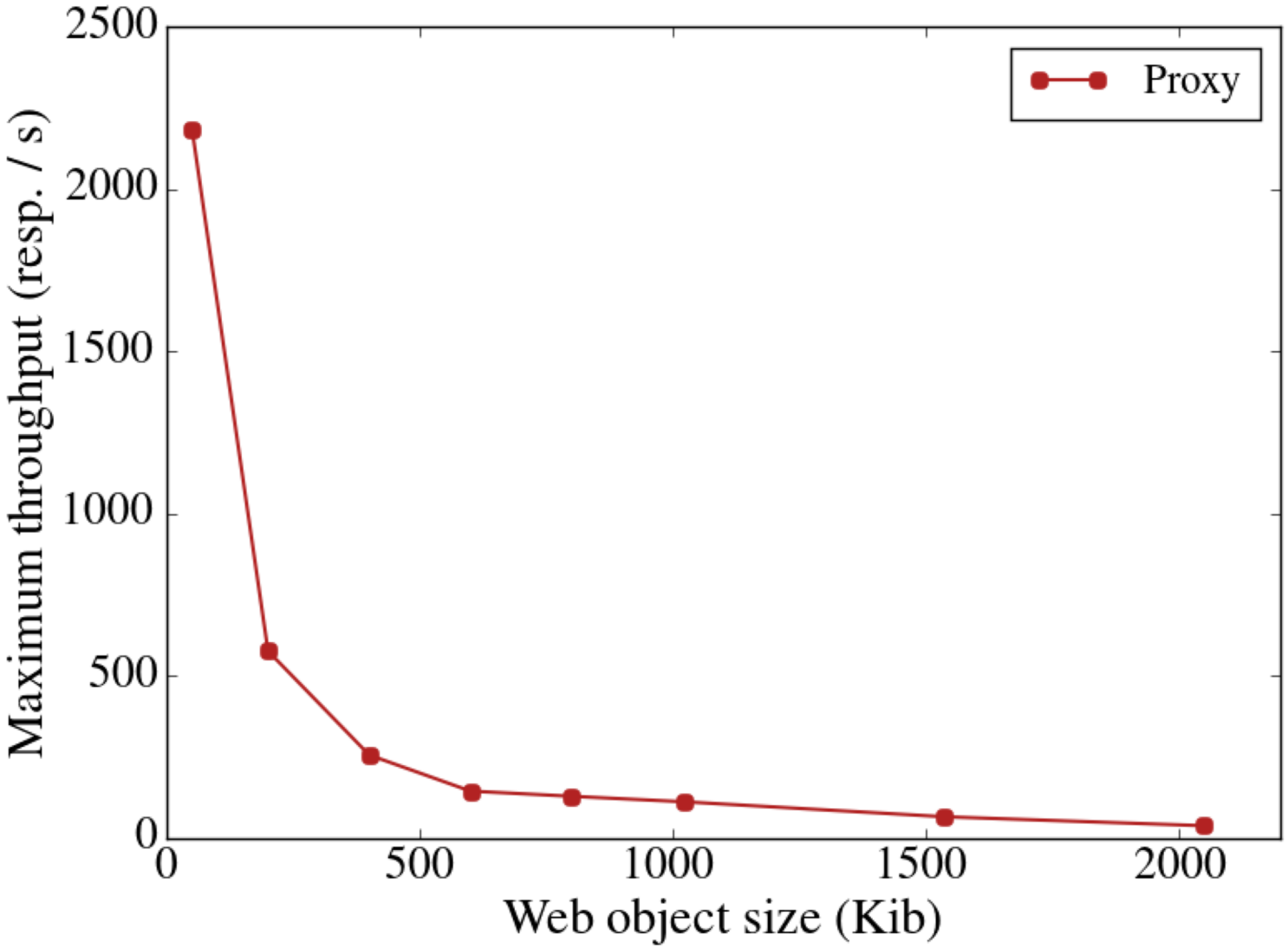
Throughput


490.5
450.9
325.8
HTTPS
HTTPS with client auth.
PoPSiCl
Response rate (resp./s)
Request rate (req./s)
0
100
200
300
400
500
600

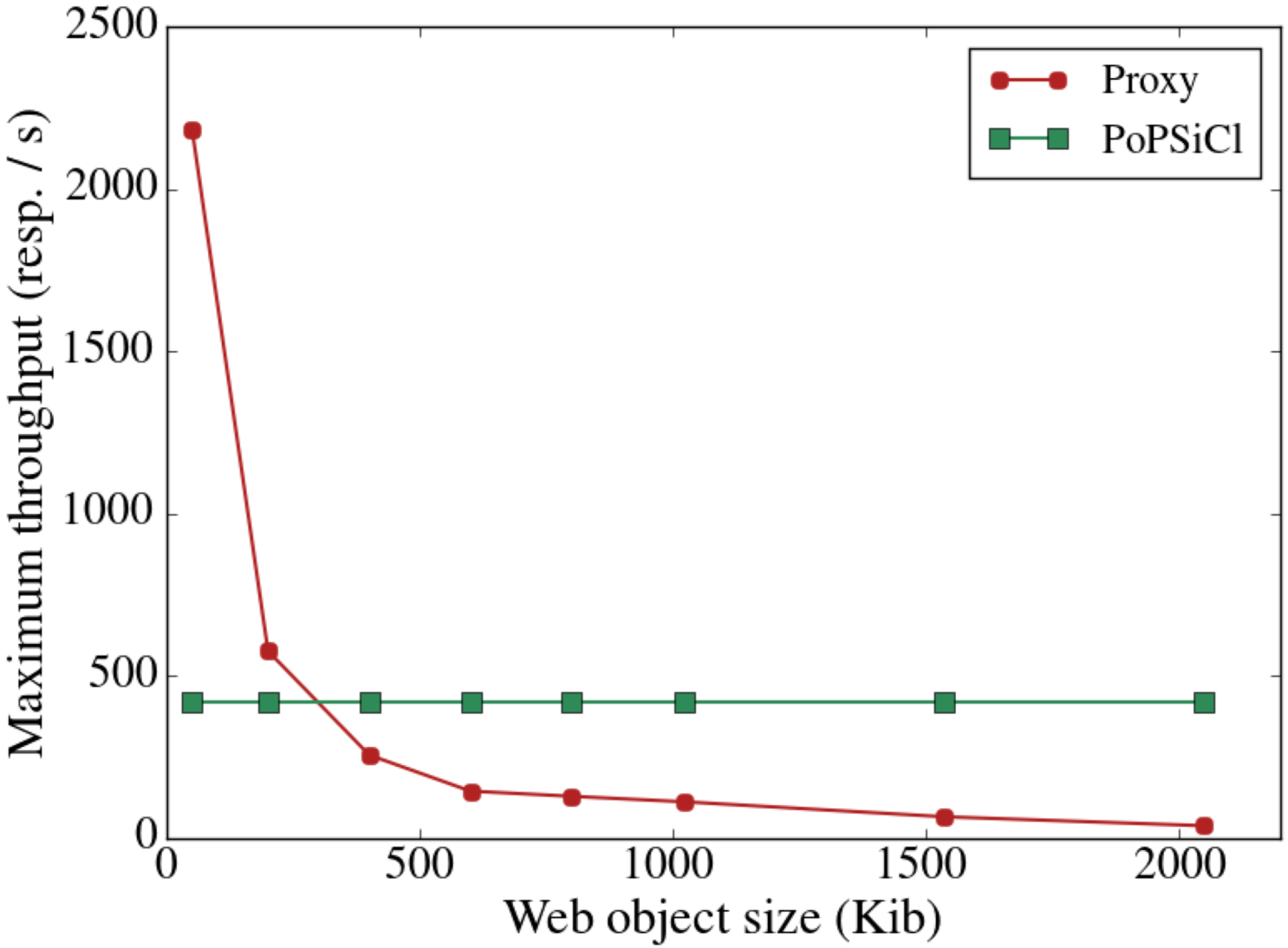
Scalability: Throughput per retrieved object size



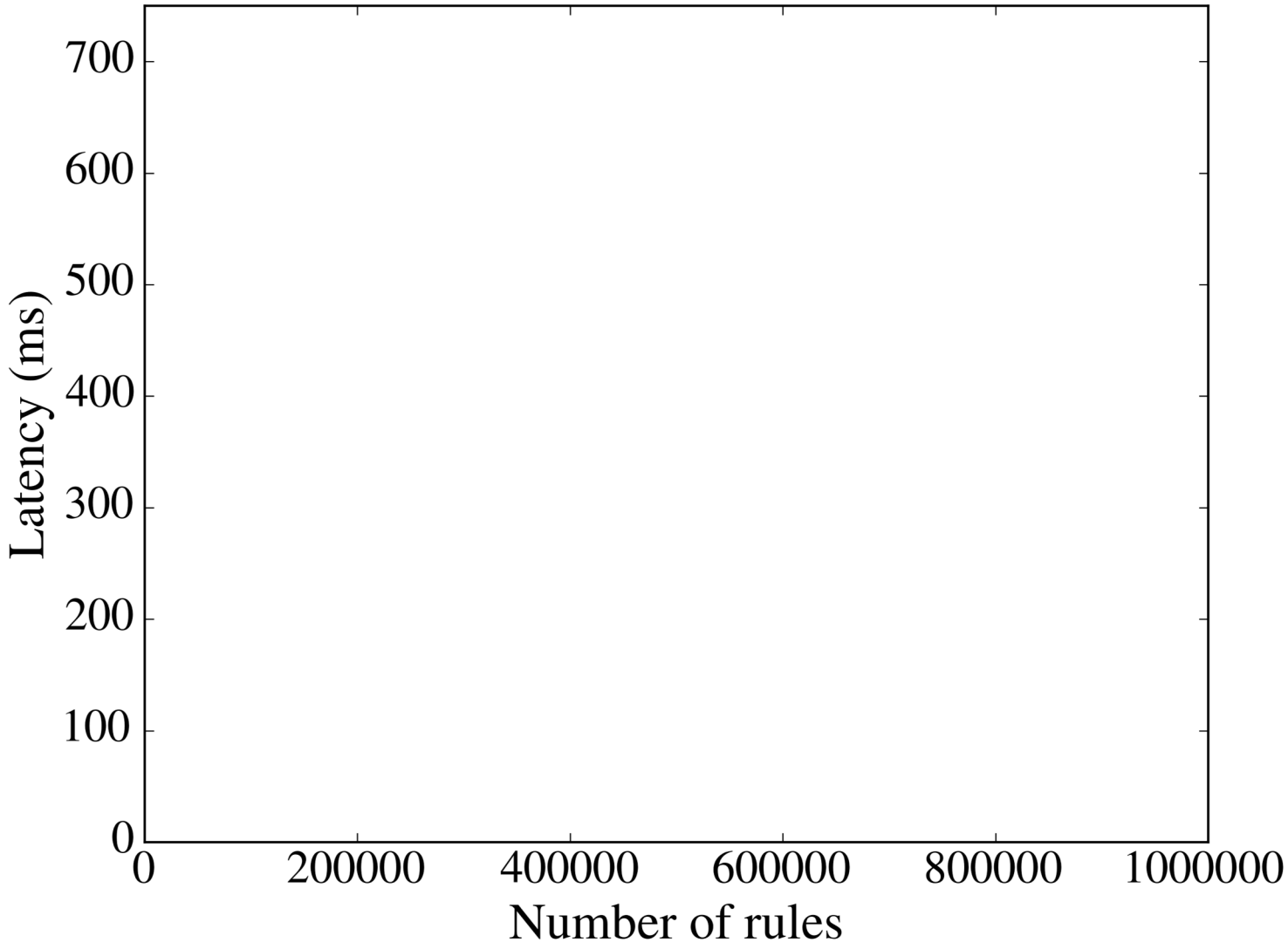
Scalability: Throughput per retrieved object size



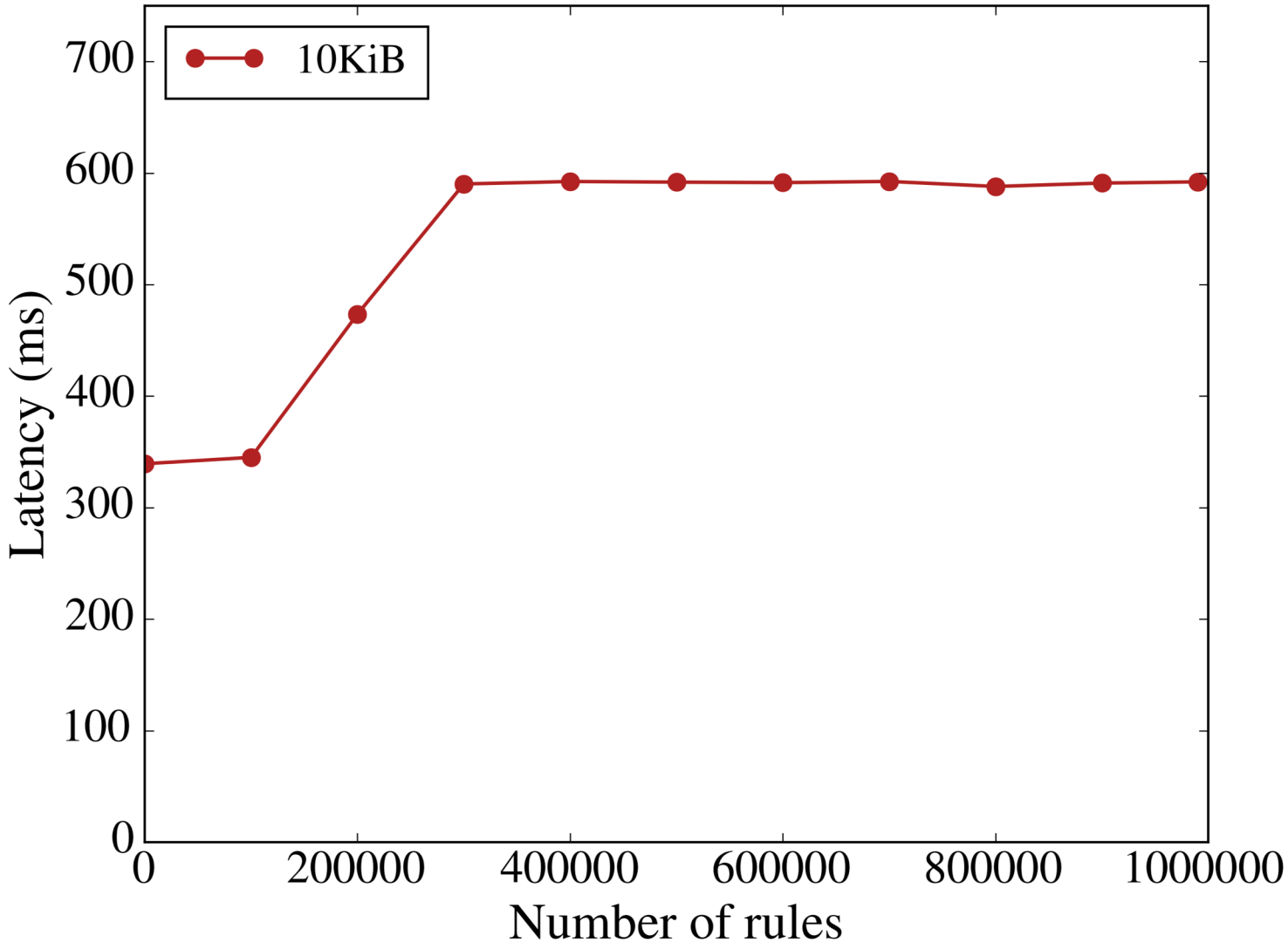
Scalability: Throughput per retrieved object size



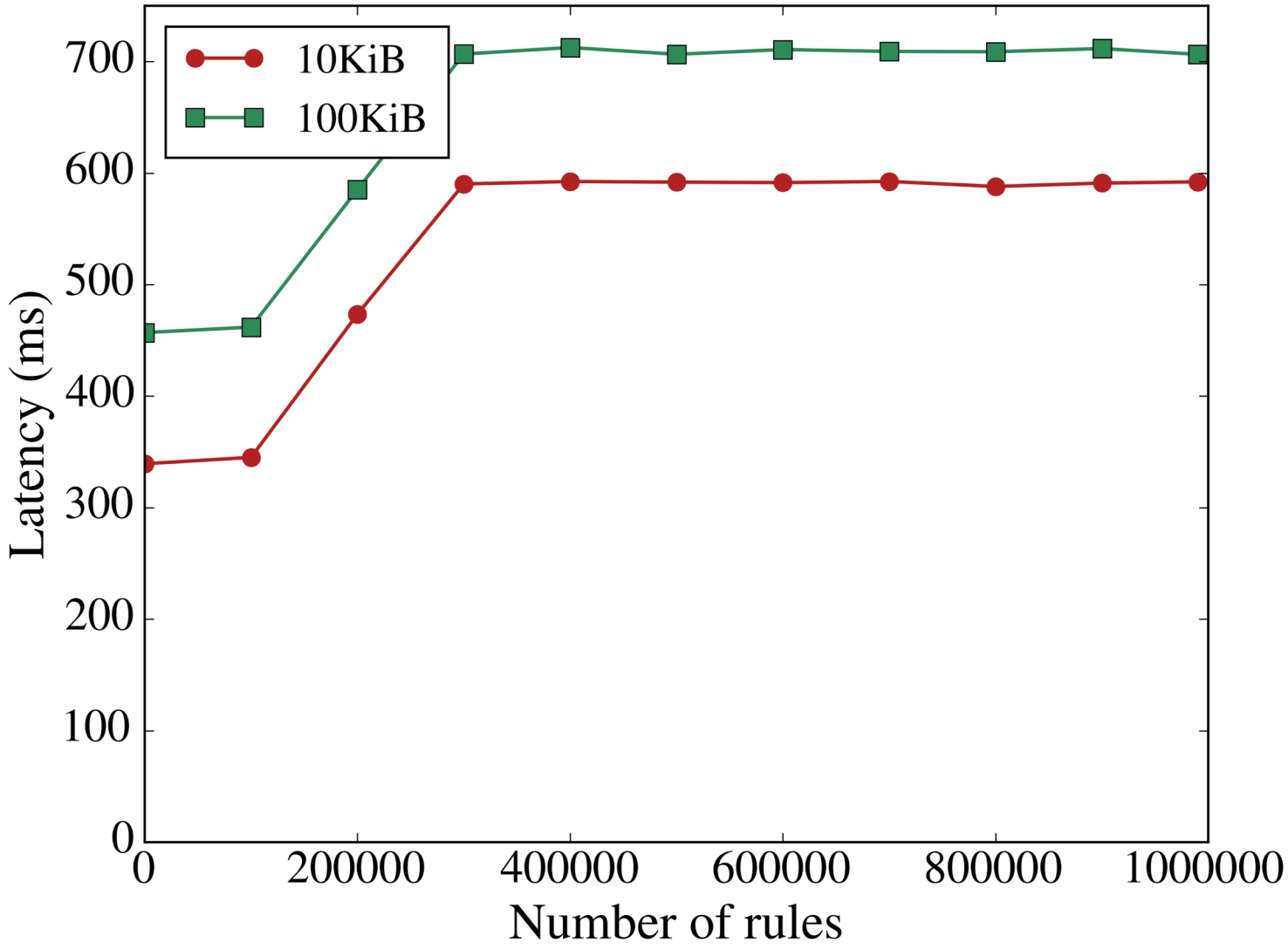
Scalability: Latency per # switch rules



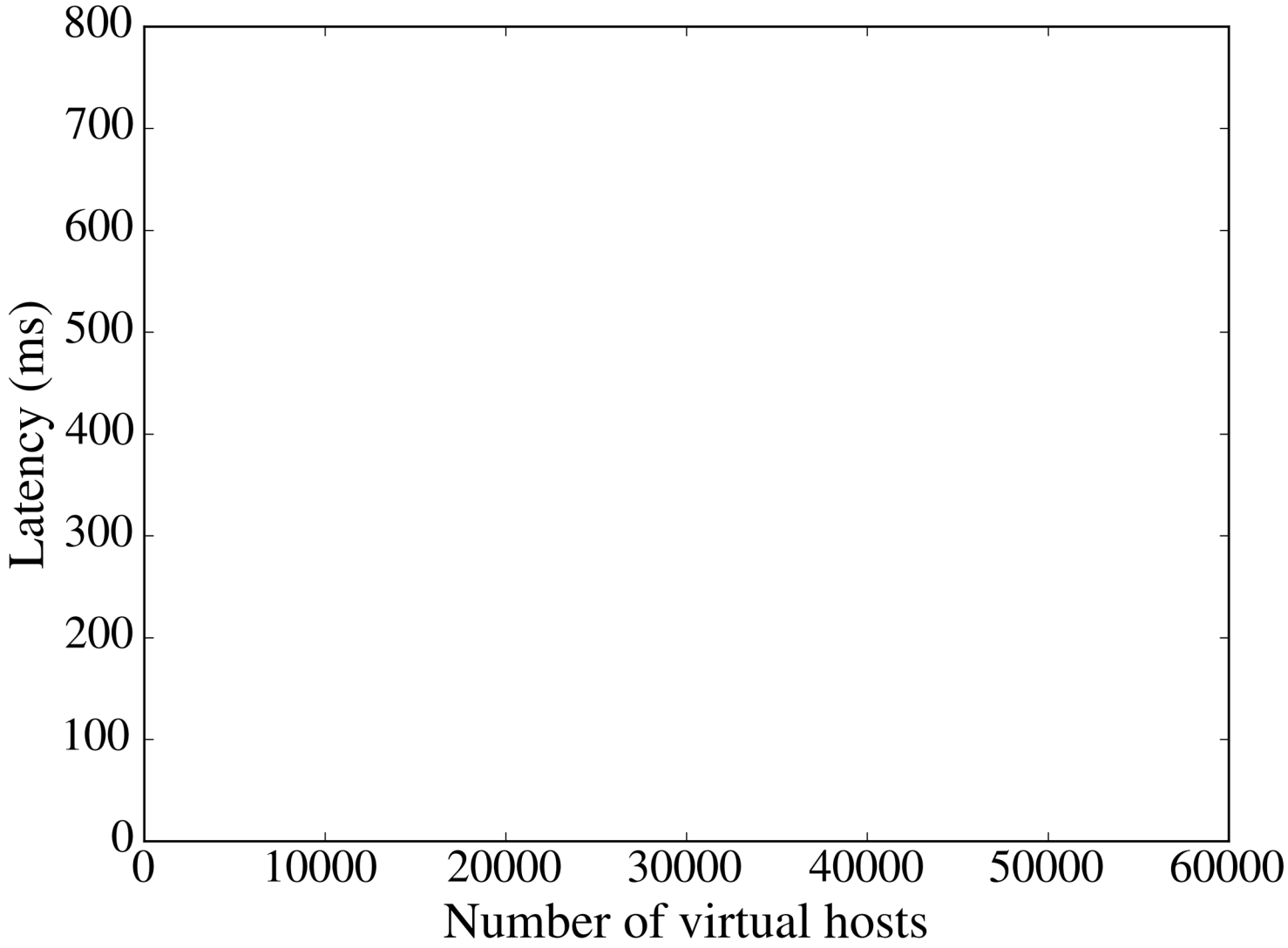
Scalability: Latency per # switch rules



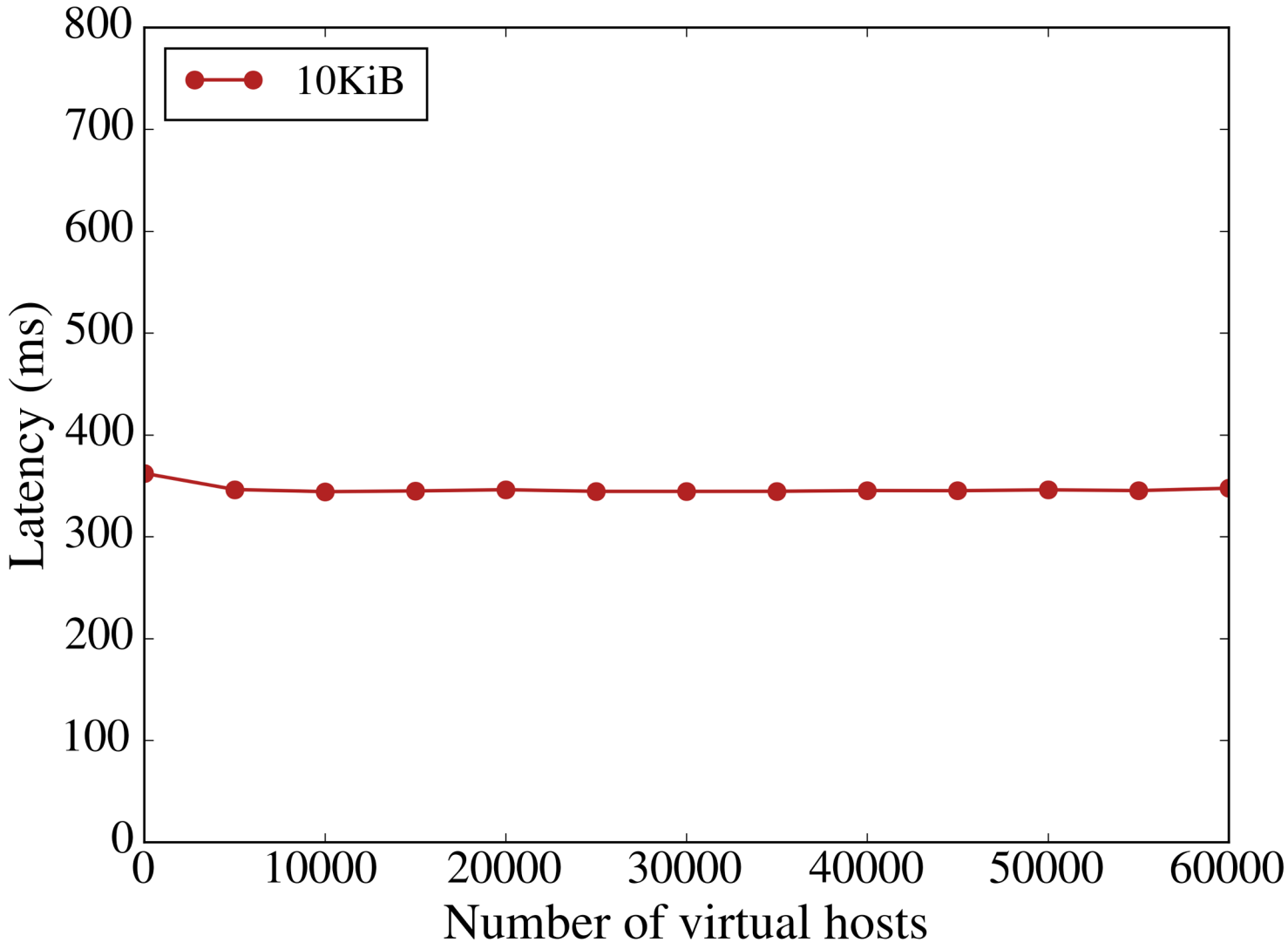
Scalability: Latency per # switch rules



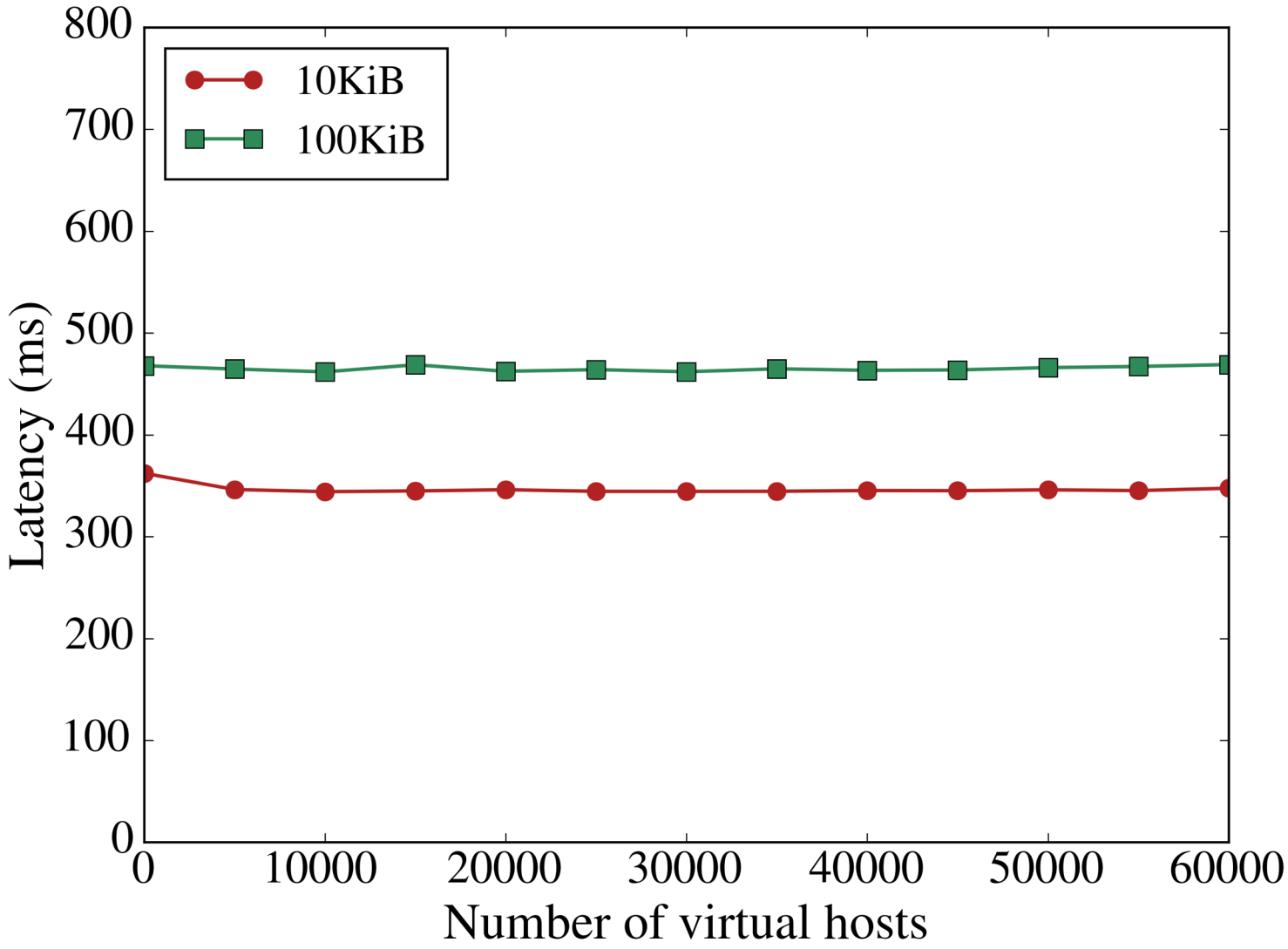
Scalability: Latency per # PoPSiCls for one server



Scalability: Latency per # PoPSiCls for one server



Scalability: Latency per # PoPSiCls for one server



Q&A