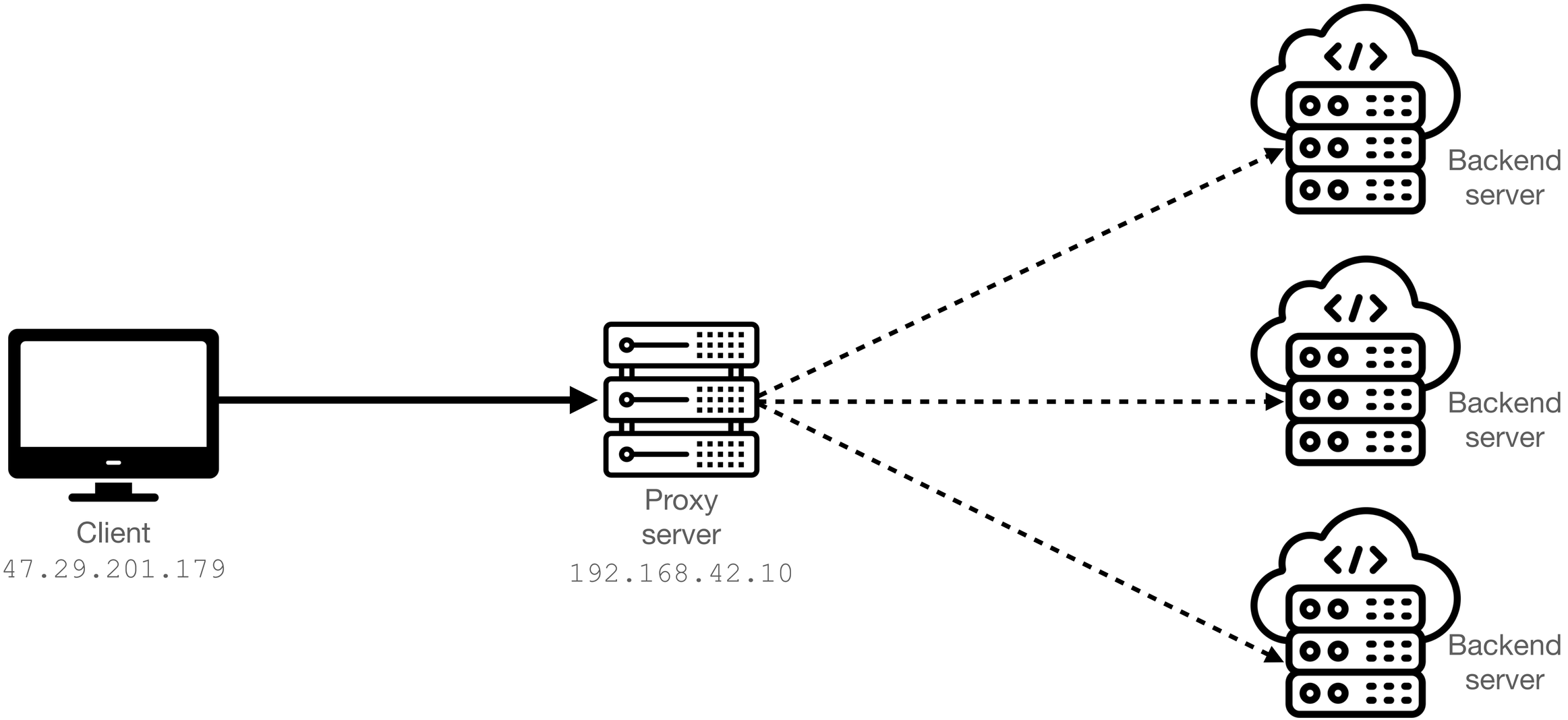
A Large-Scale Measurement Study of the PROXY Protocol and its Security Implications

Stijn Pletinckx, Christopher Kruegel, Giovanni Vigna

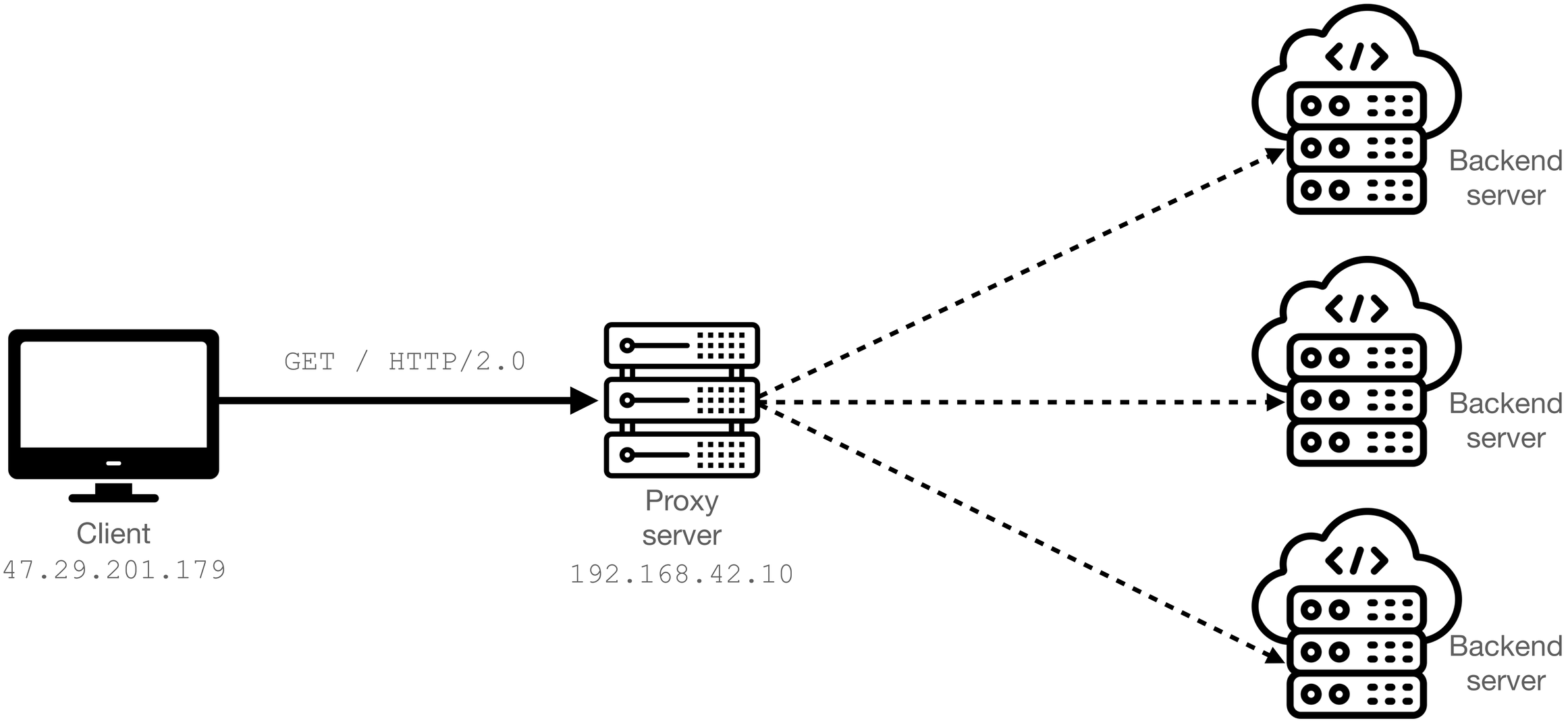
University of California, Santa Barbara

SECLAB

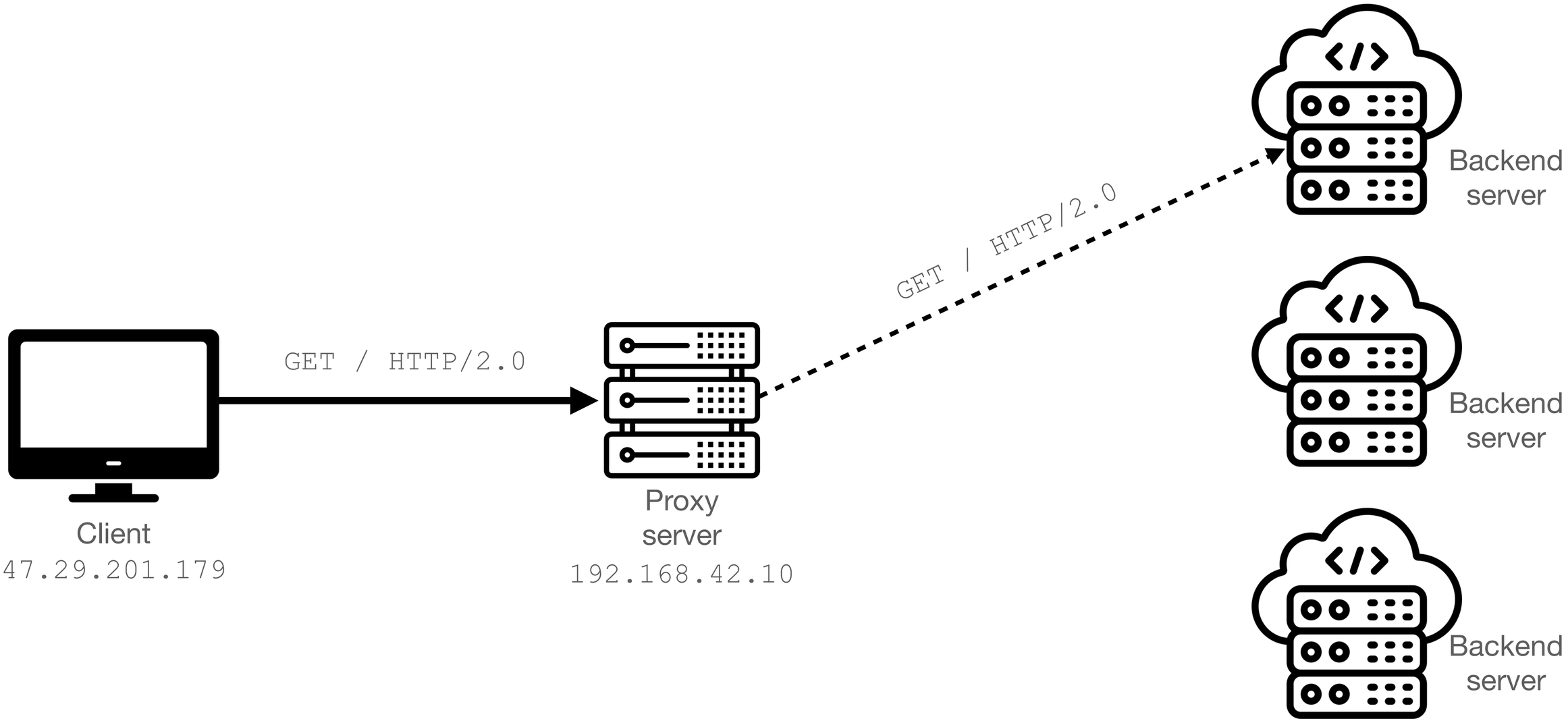
(Reverse) Proxy Servers



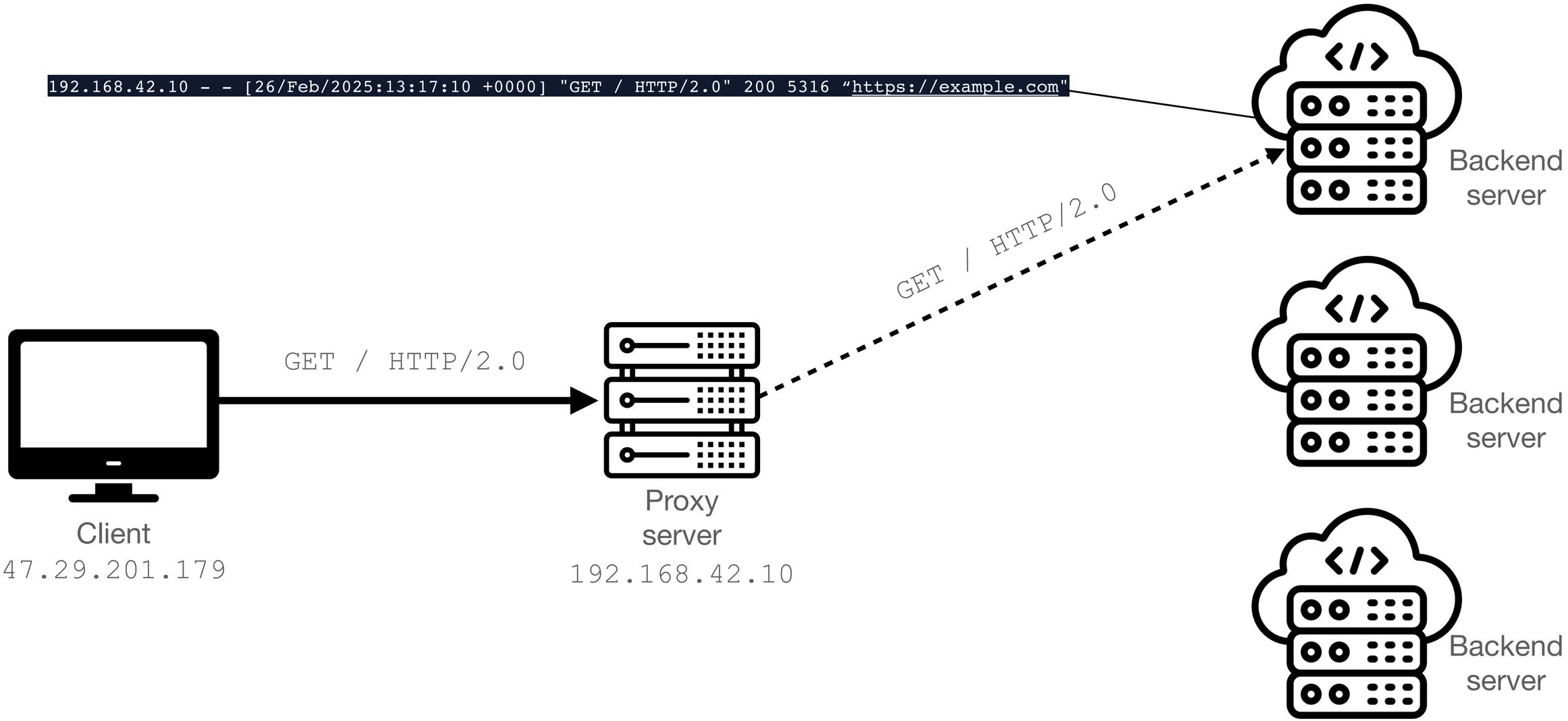
(Reverse) Proxy Servers



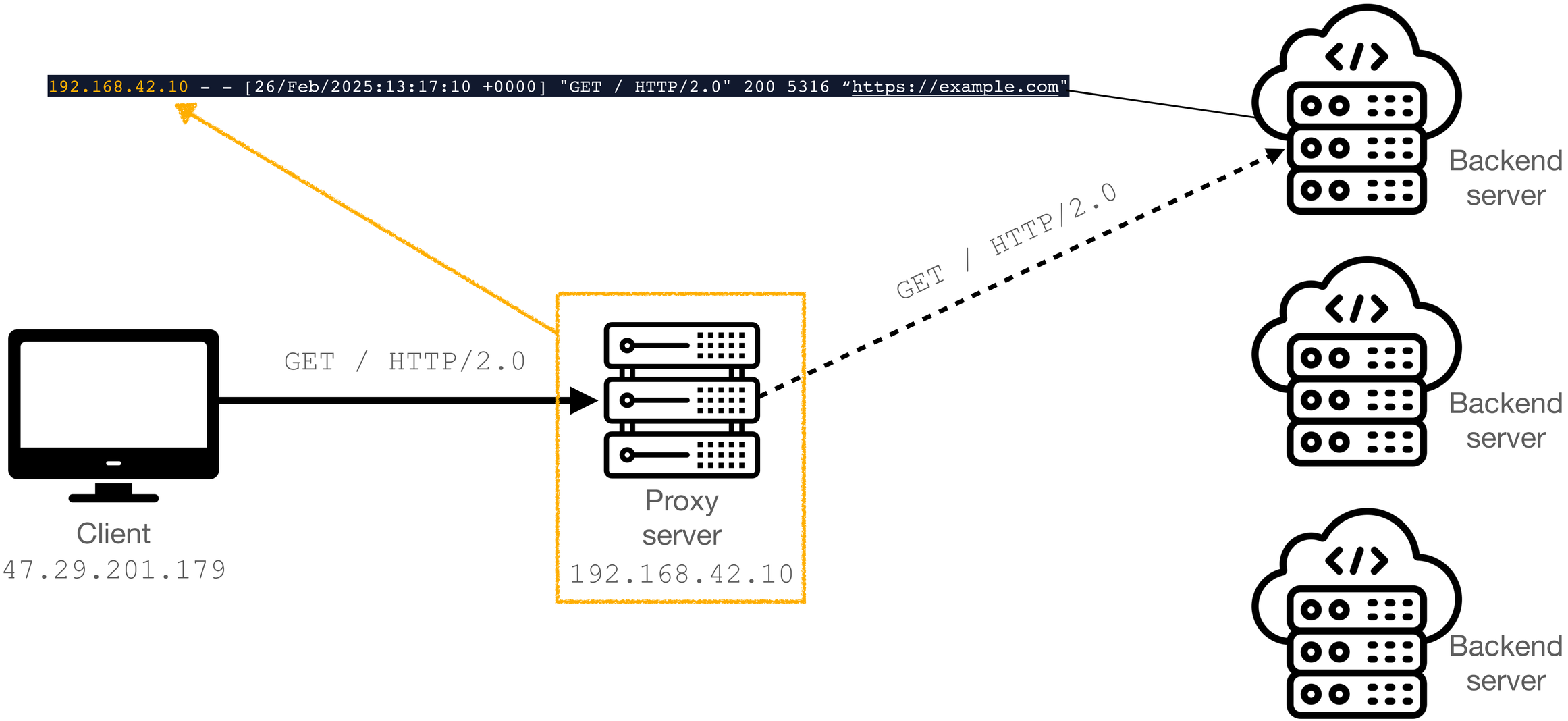
(Reverse) Proxy Servers



(Reverse) Proxy Servers



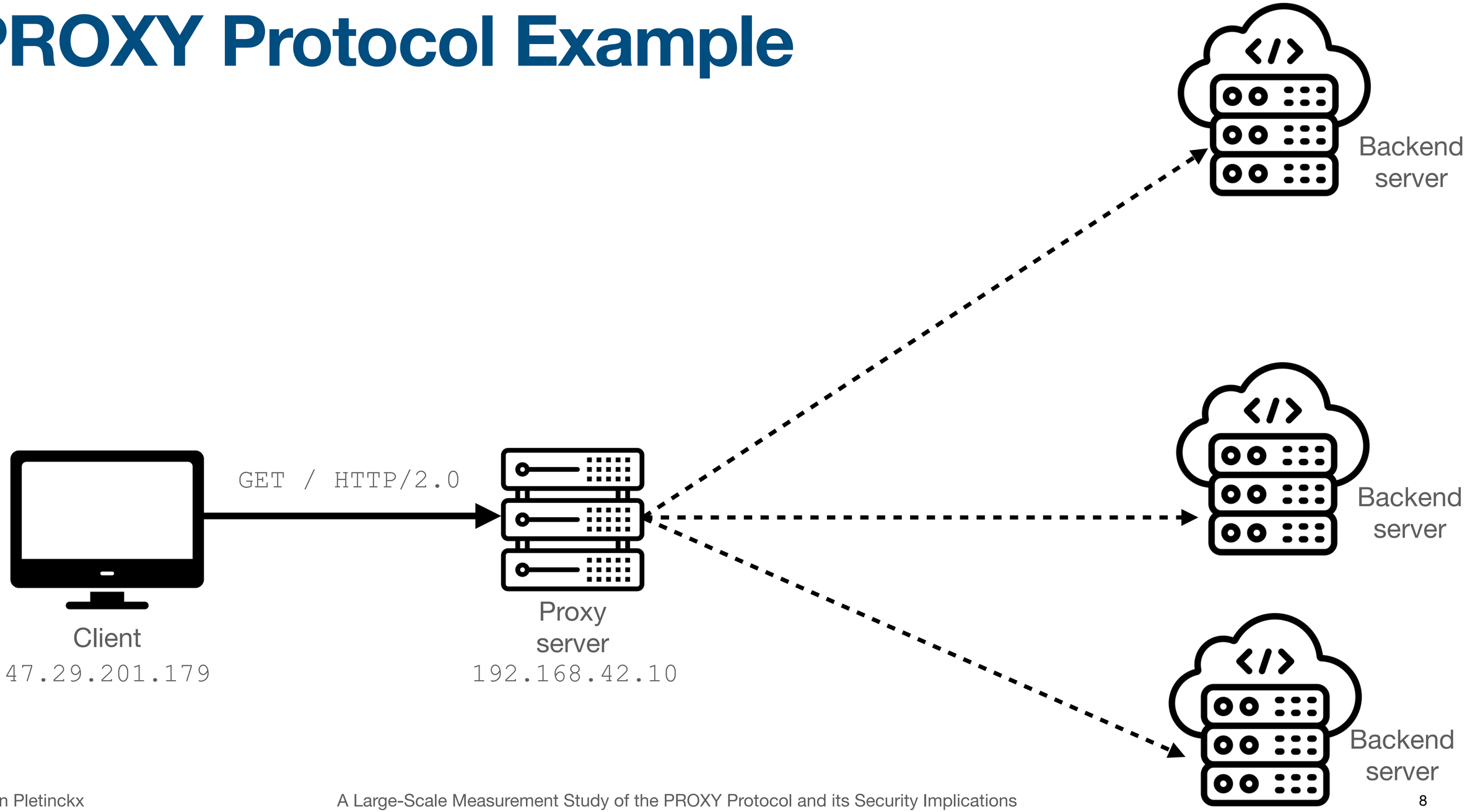
(Reverse) Proxy Servers



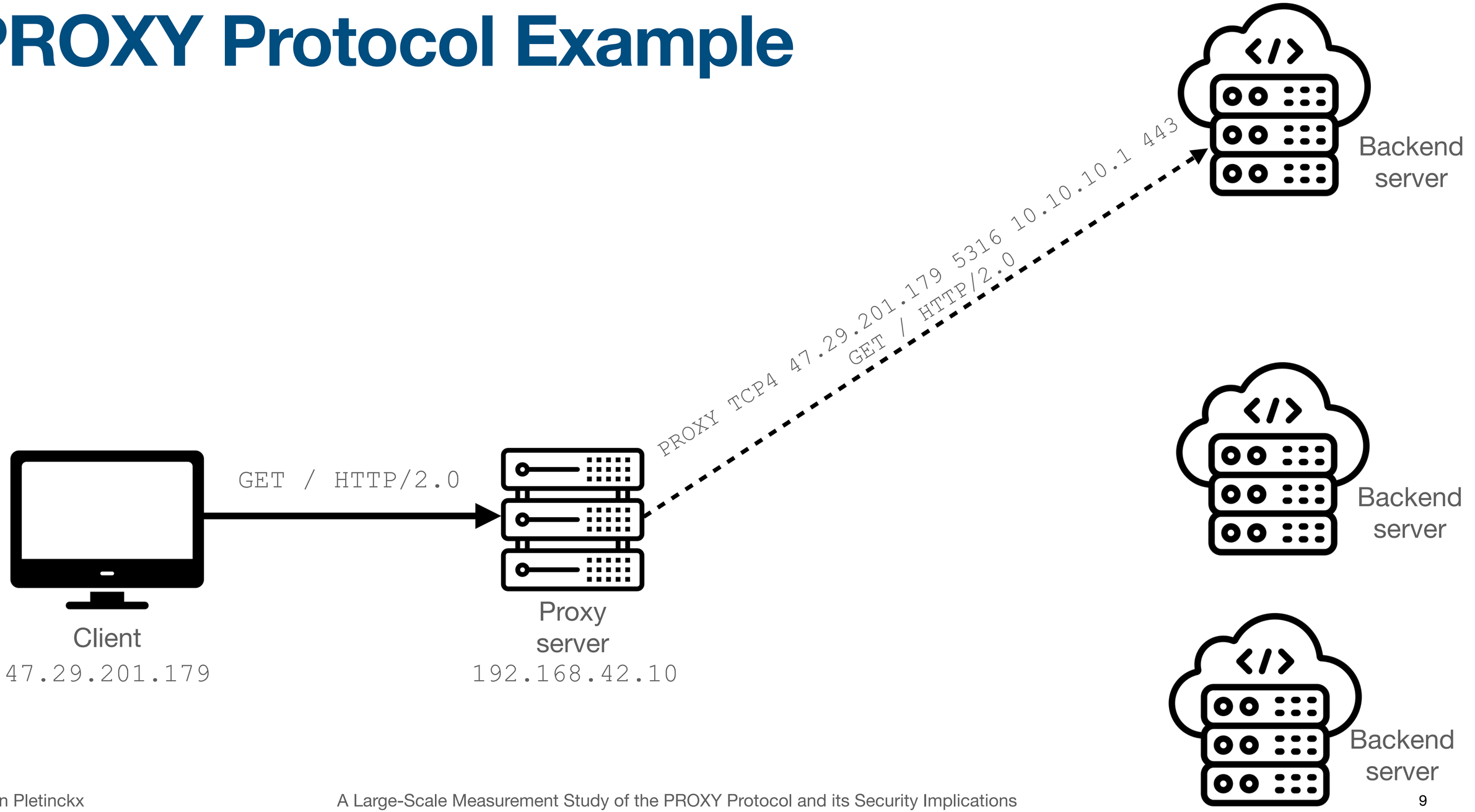
The PROXY Protocol

- Convey client information from the proxy server to the backend server
- Application agnostic (protocol interacts on layer 4)
- Appends PROXY header during connection setup

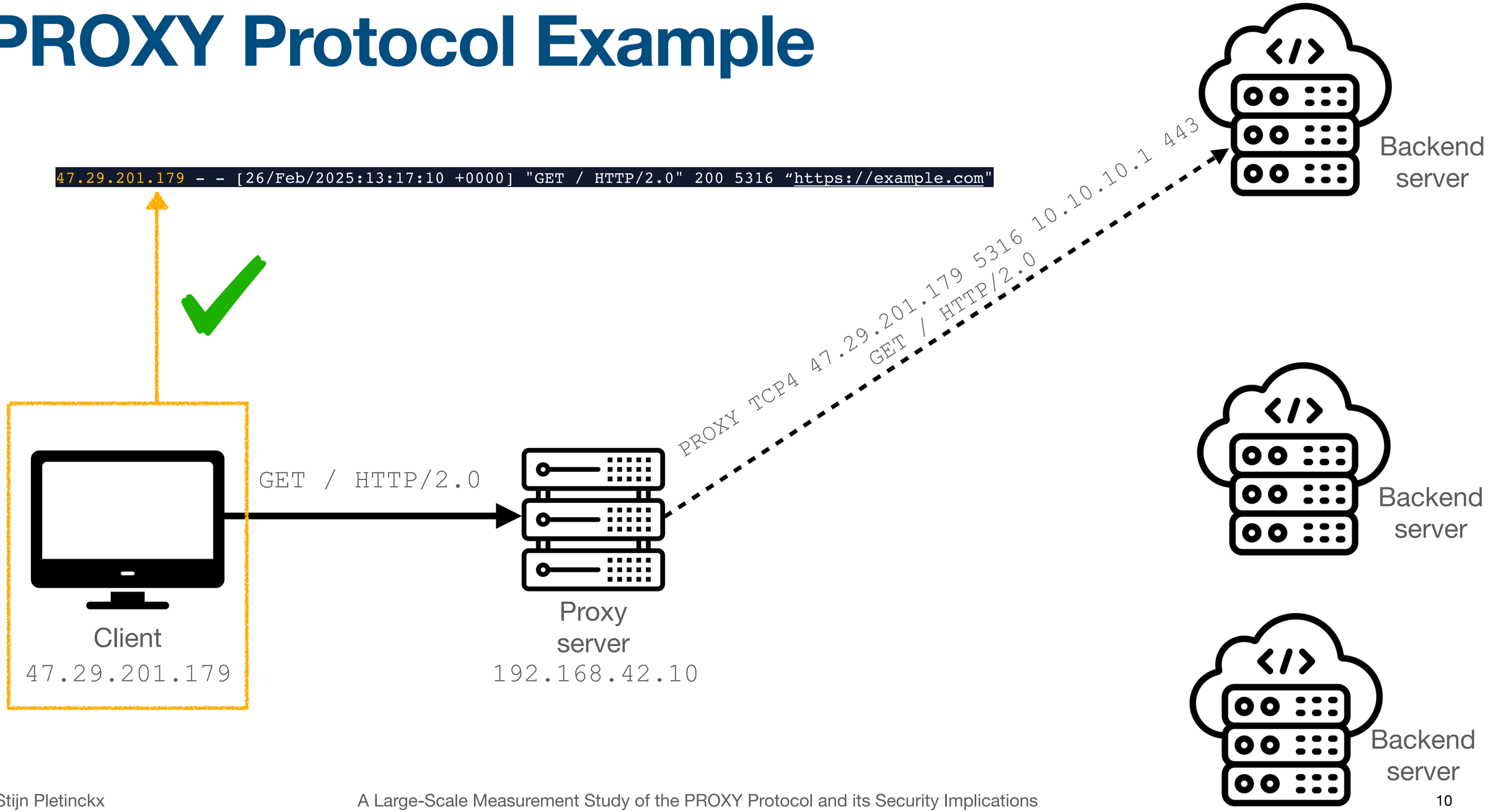
PROXY Protocol Example



PROXY Protocol Example



PROXY Protocol Example

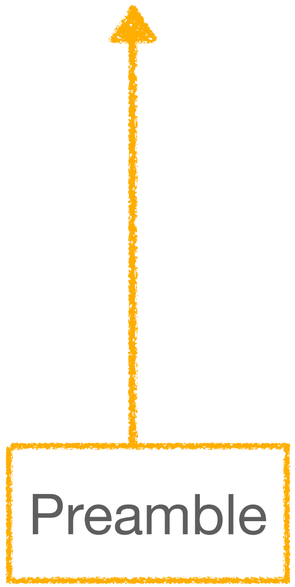


The PROXY Header (v1)

```
PROXY   TCP4   47.29.201.179   5316   10.10.10.1   443
```

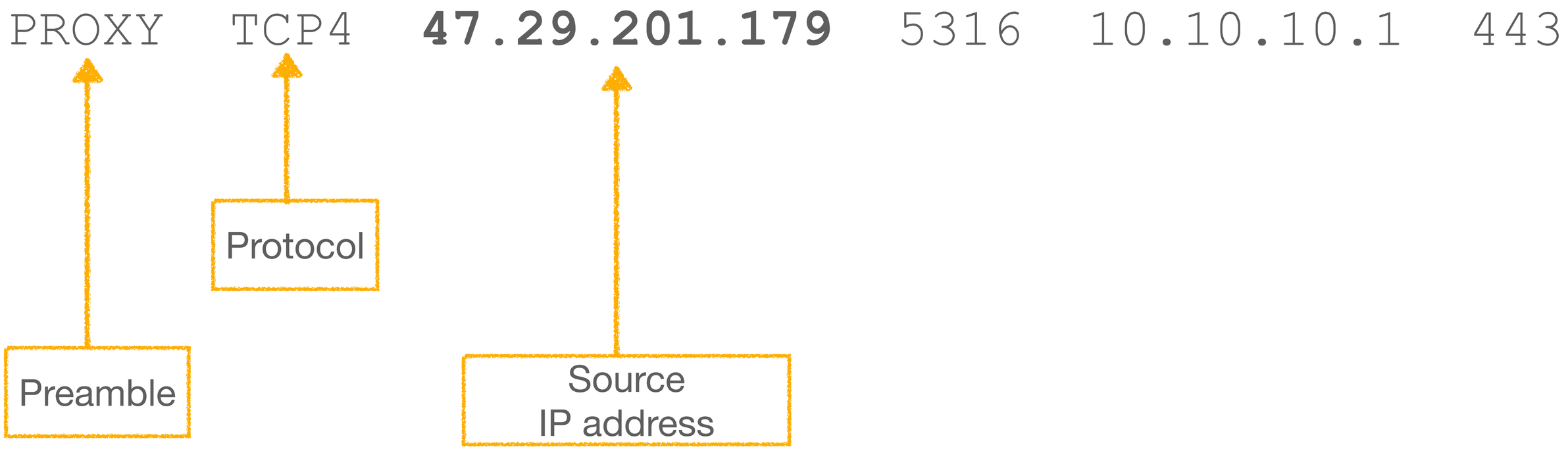
The PROXY Header (v1)

```
PROXY   TCP4   47.29.201.179   5316   10.10.10.1   443
```

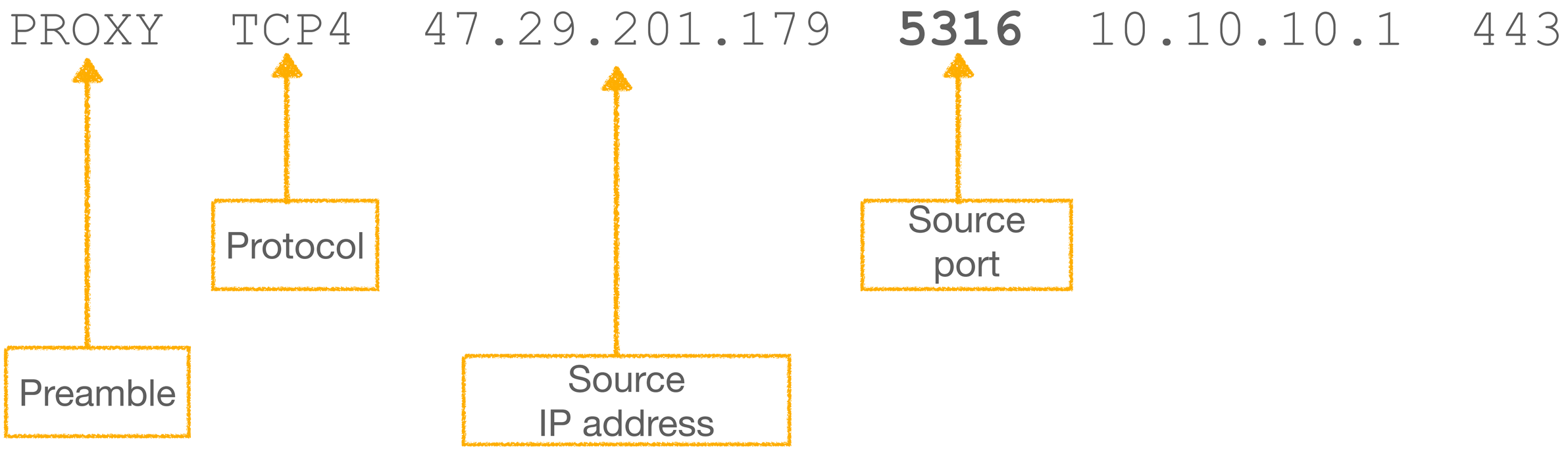


The PROXY Header (v1)

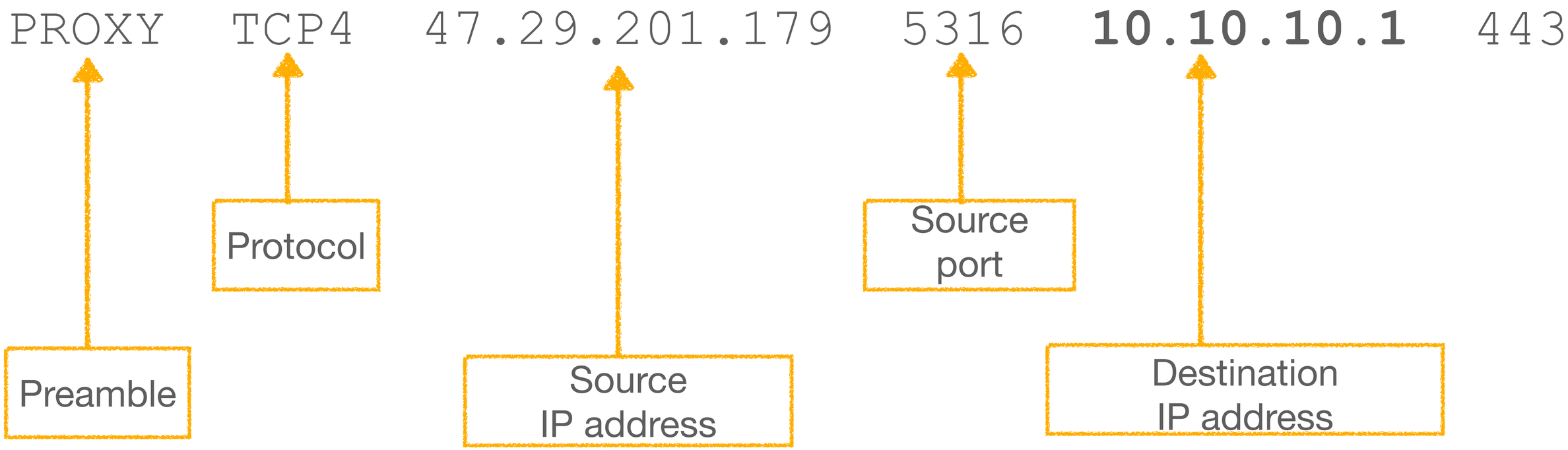
The PROXY Header (v1)



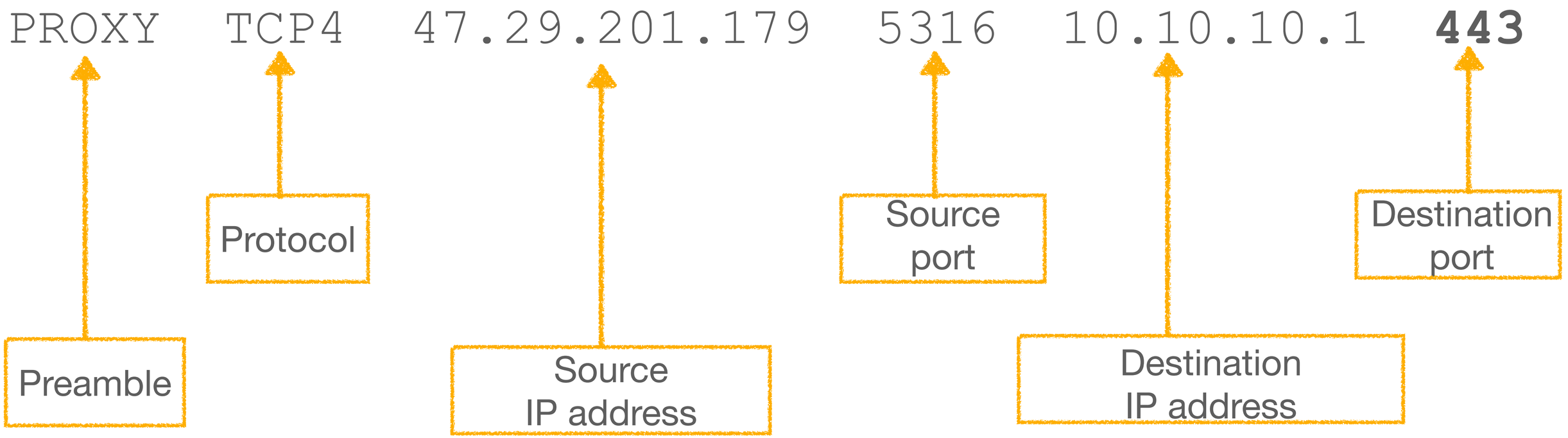
The PROXY Header (v1)



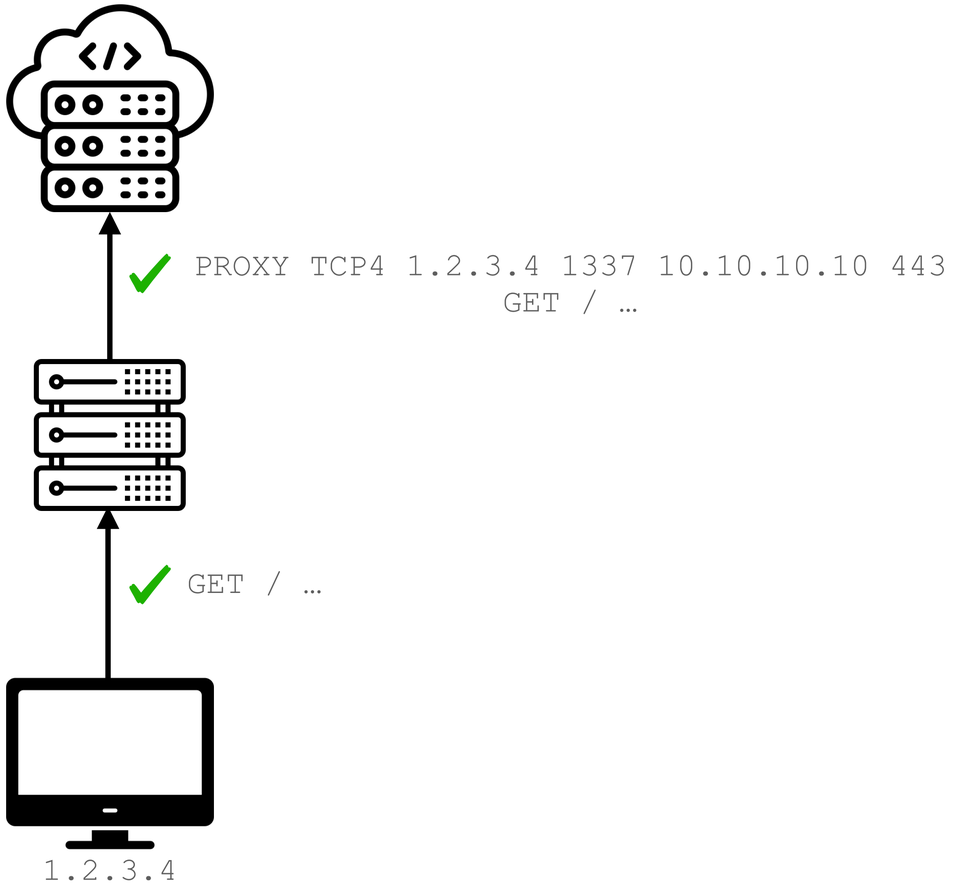
The PROXY Header (v1)



The PROXY Header (v1)

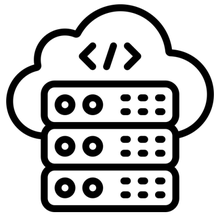


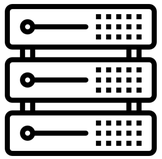
PROXY Protocol and Security



- Access control
- Denial of Service (DoS) protection
- Central blocklisting

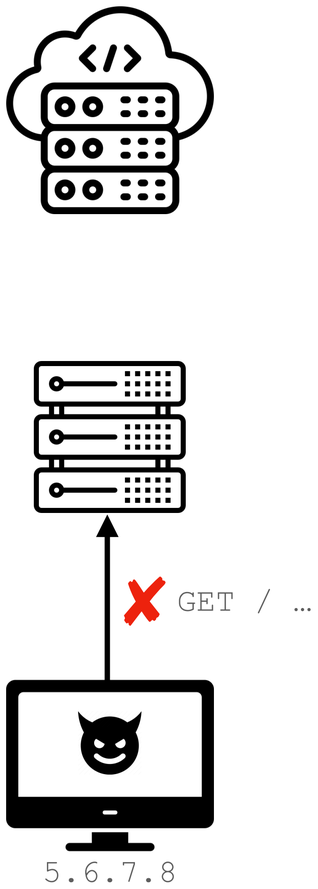
PROXY Protocol and Security



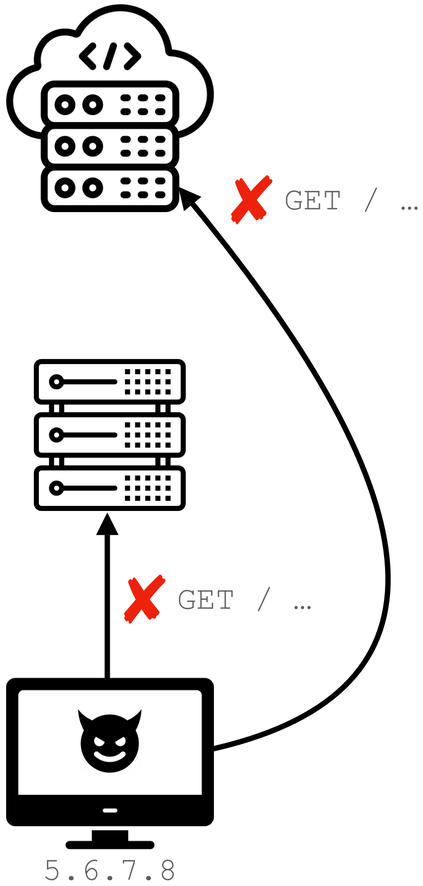


5.6.7.8

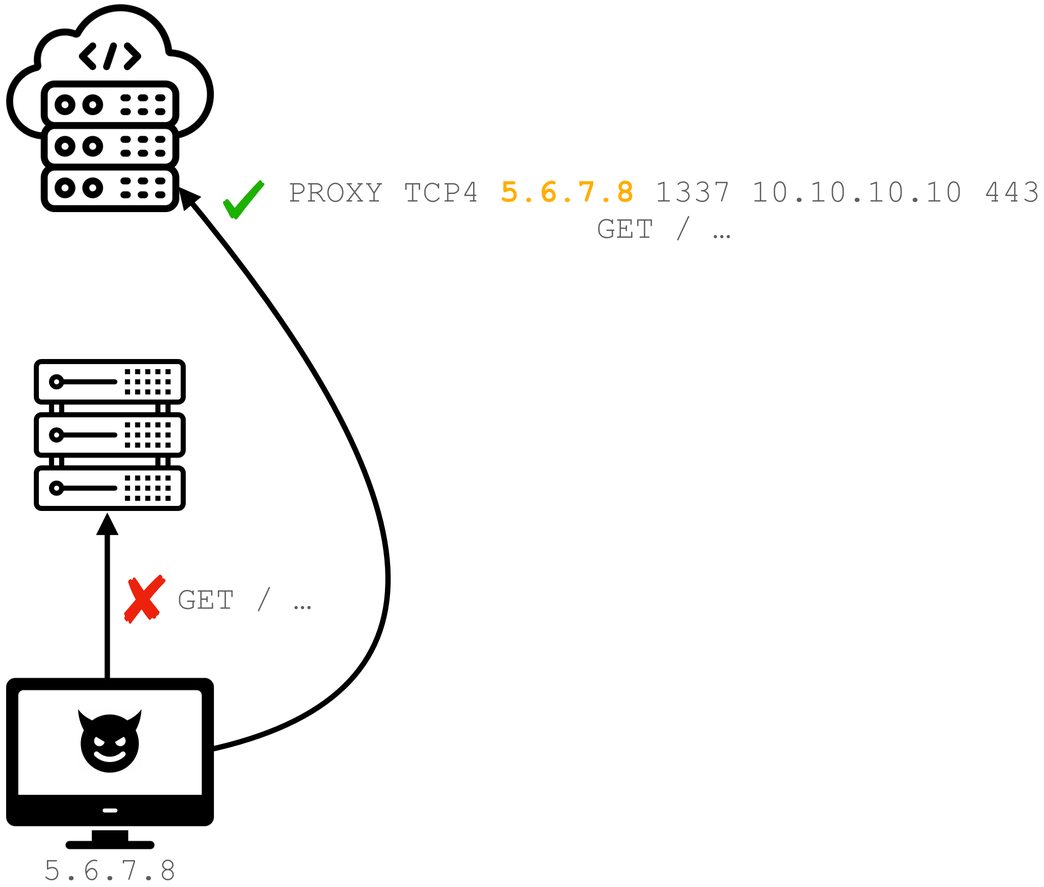
PROXY Protocol and Security



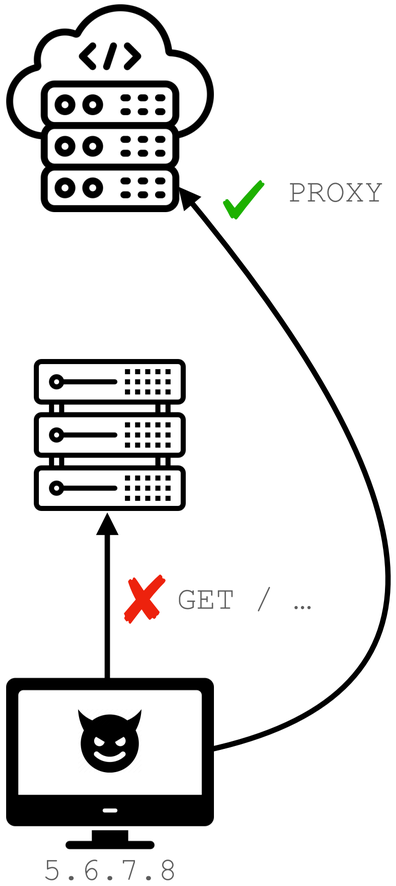
PROXY Protocol and Security



PROXY Protocol and Security

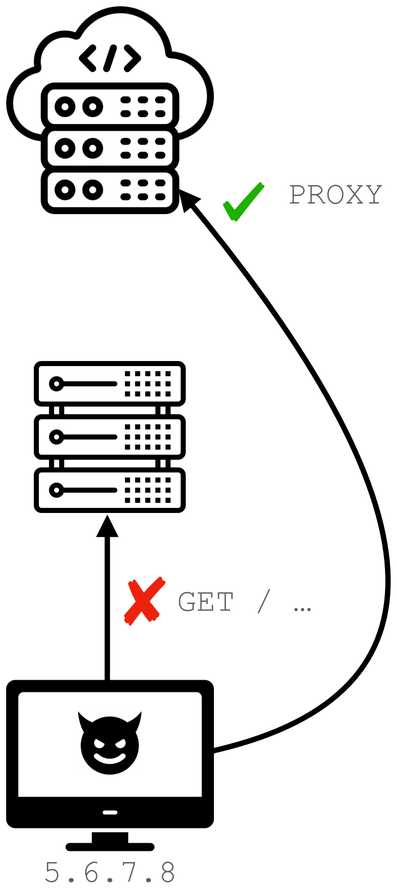


PROXY Protocol and Security

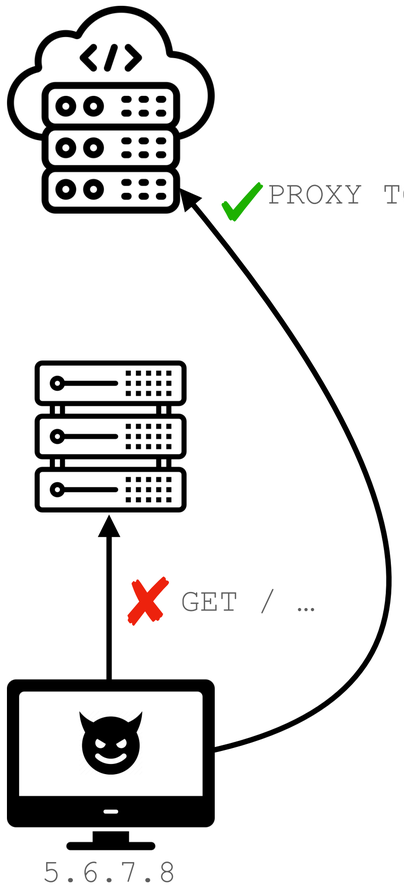


1. **Administrator does not configure a firewall rule for the PROXY Protocol**
2. **Backend server does not perform IP-based access control**

PROXY Protocol and Security

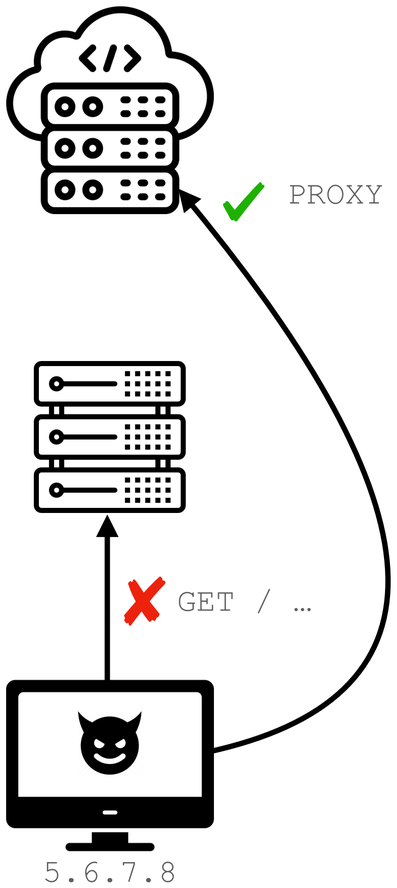


1. **Administrator does not configure a firewall rule for the PROXY Protocol**
2. **Backend server does not perform IP-based access control**



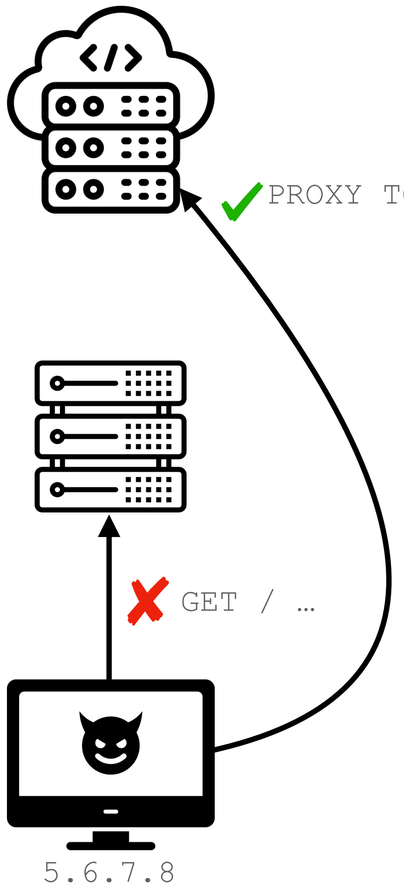
Backend server does perform IP-based access control, but we can circumvent it by spoofing the source IP value in the PROXY header

PROXY Protocol and Security



1. **Administrator does not configure a firewall rule for the PROXY Protocol**
2. **Backend server does not perform IP-based access control**

Regular bypass



Backend server does perform IP-based access control, but we can circumvent it by spoofing the source IP value in the PROXY header

Spoofed bypass

Our Work

1. How prevalent are regular bypasses and spoofed bypasses in the wild?

2. What are the security implications of these bypasses?

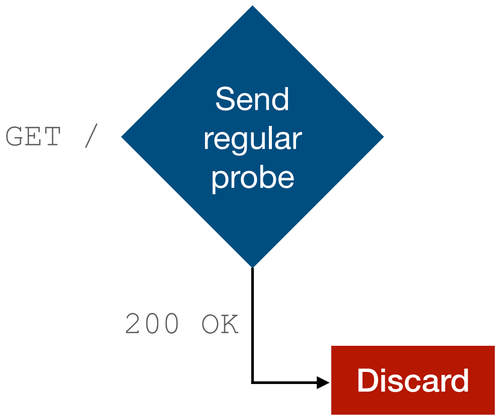
Our Method

- Large-scale measurement study on the full IPv4 address space
- Three protocols:
  - HTTP
  - SMTP
  - SSH
- Use ZMap for initial port scan, then ZGrab for full handshake

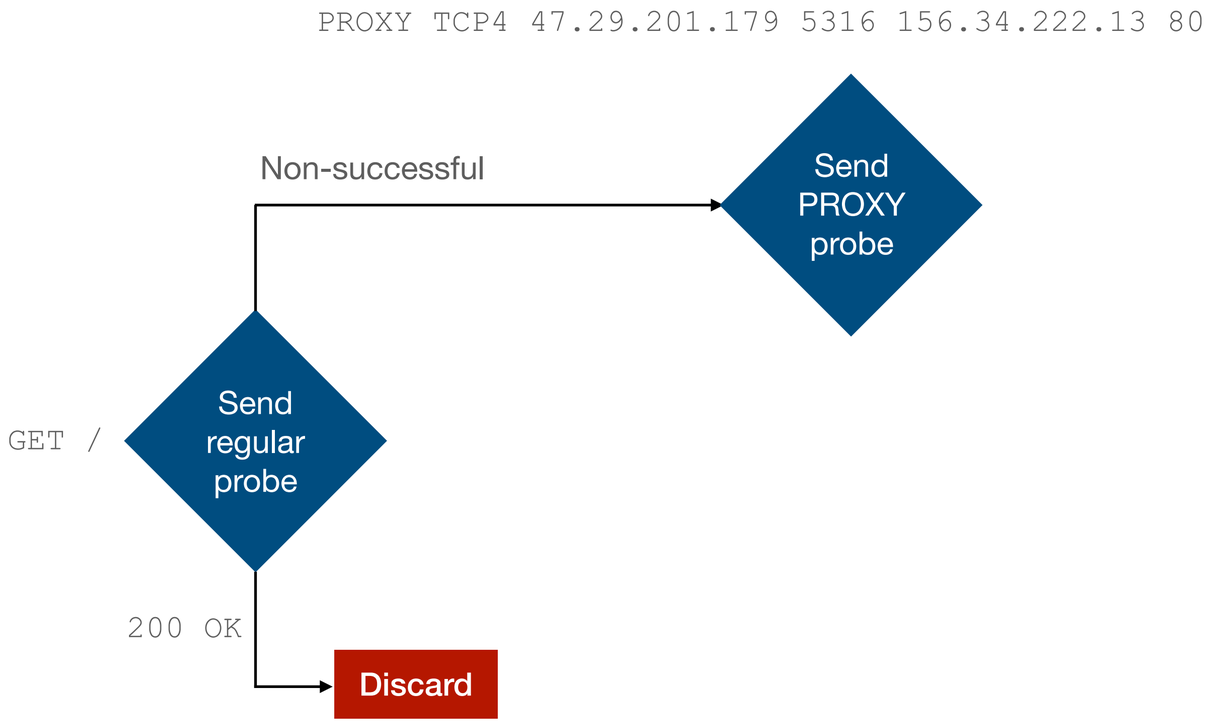
Our Method

GET /

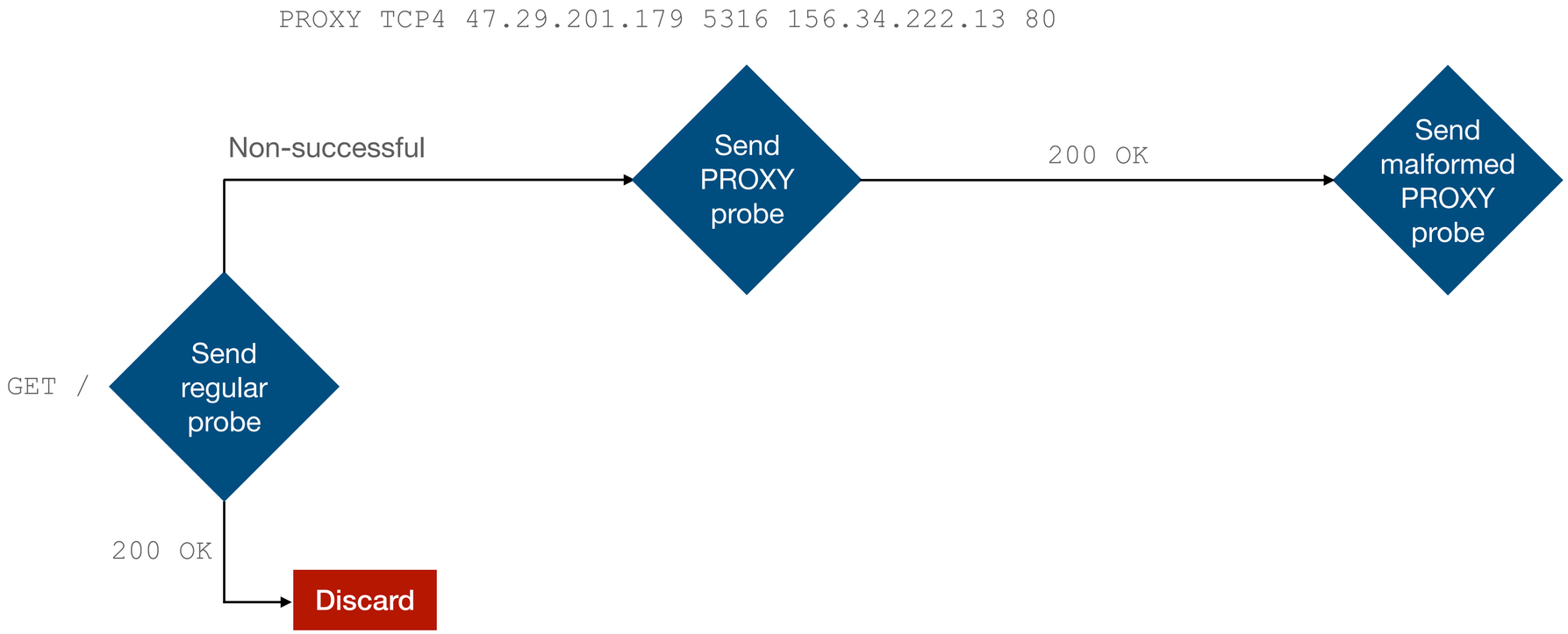
Our Method



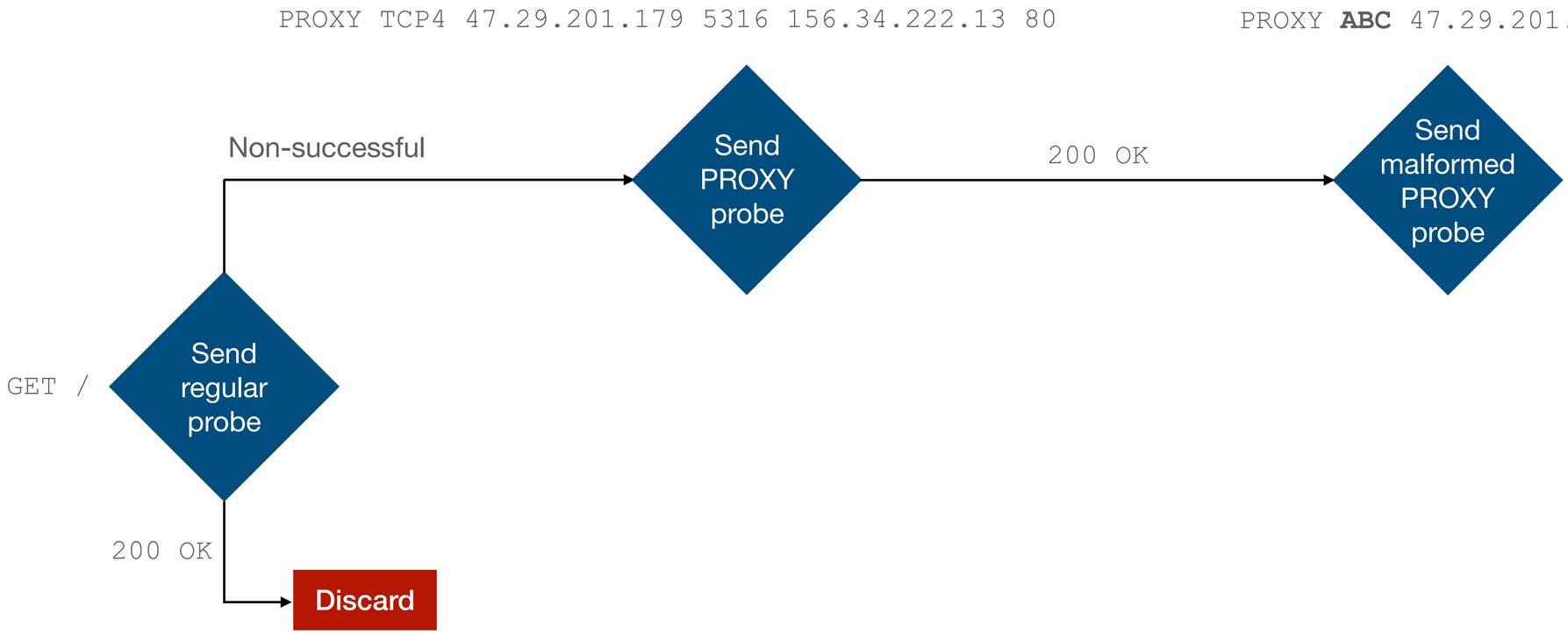
Our Method


PROXY TCP4 47.29.201.179 5316 156.34.222.13 80
Non-successful
Send PROXY probe
Send regular probe
GET /
200 OK
Discard

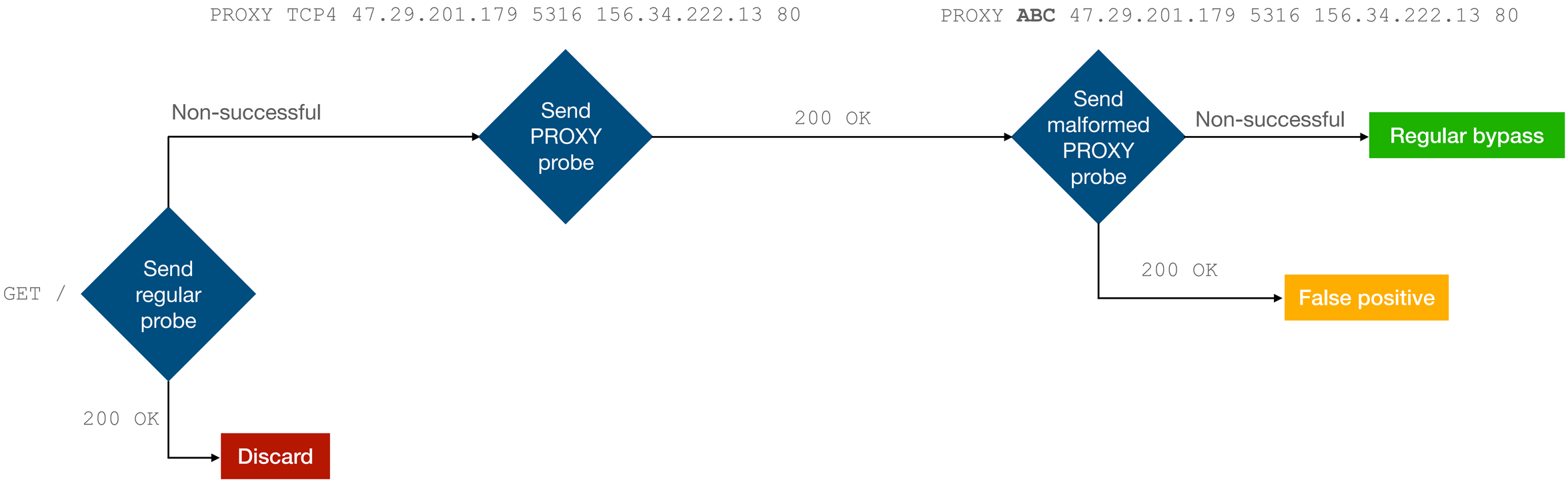
Our Method


PROXY TCP4 47.29.201.179 5316 156.34.222.13 80
Non-successful
Send PROXY probe
200 OK
Send malformed PROXY probe
GET /
Send regular probe
200 OK
Discard

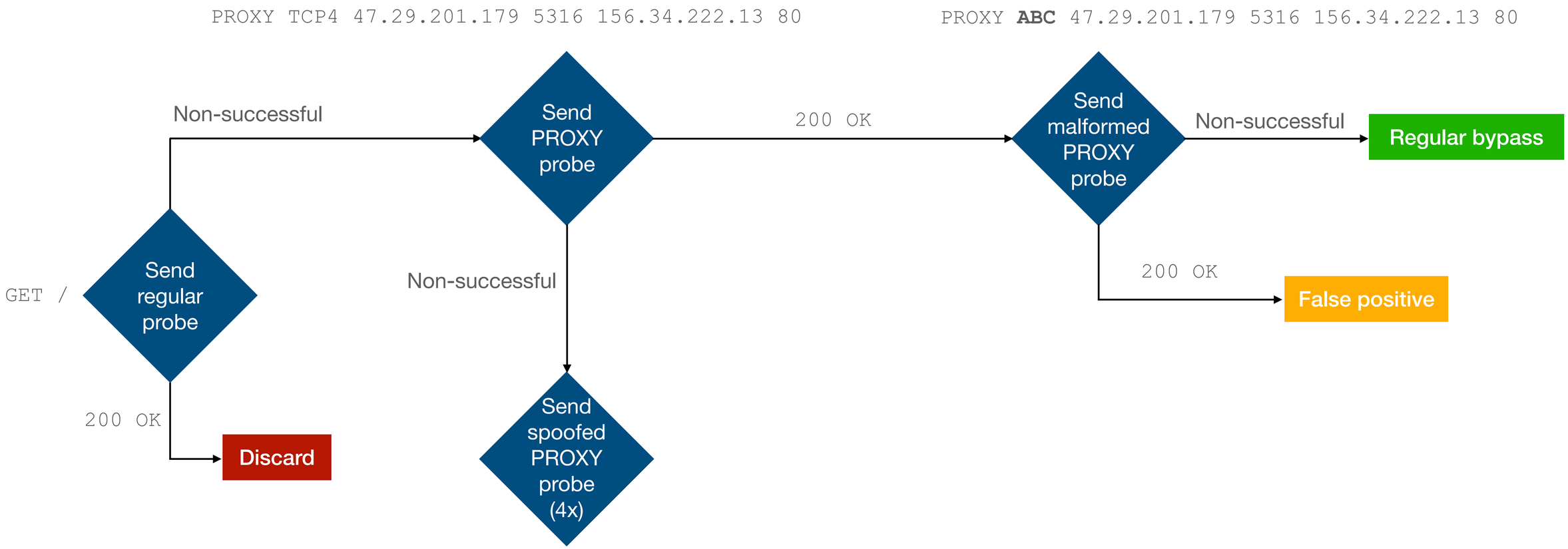
Our Method


PROXY TCP4 47.29.201.179 5316 156.34.222.13 80
PROXY ABC 47.29.201.179 5316 156.34.222.13 80
Non-successful
Send PROXY probe
200 OK
Send malformed PROXY probe
GET /
Send regular probe
200 OK
Discard

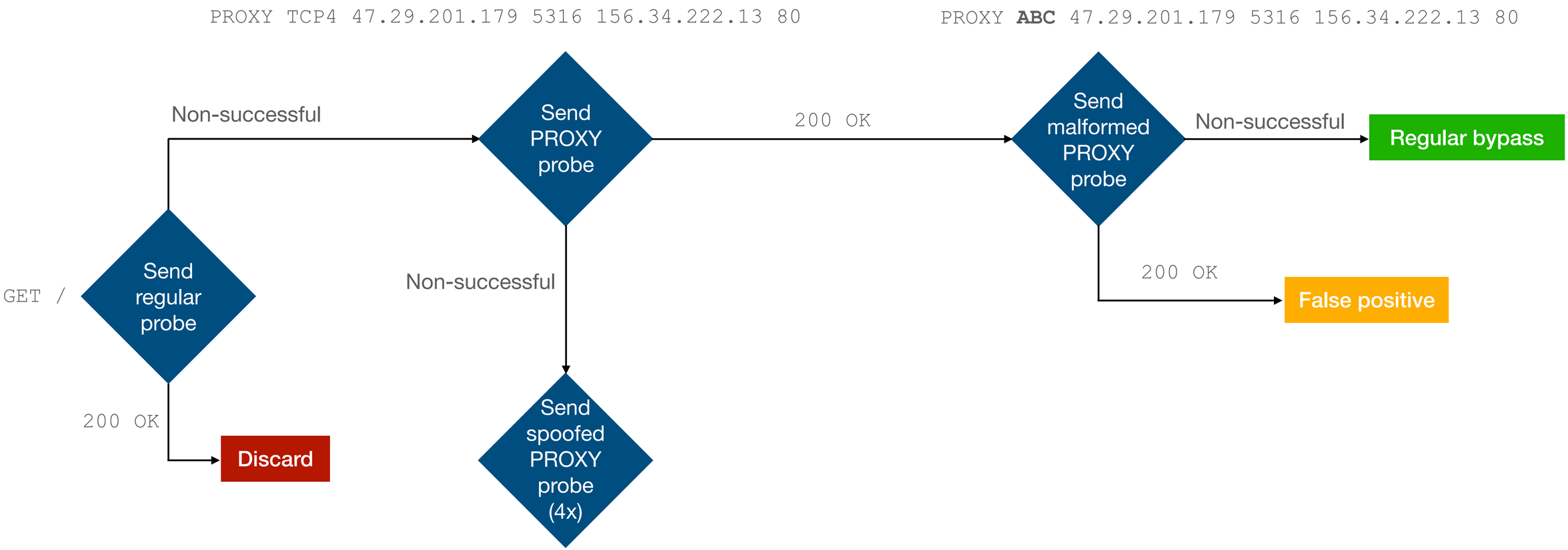
Our Method


PROXY TCP4 47.29.201.179 5316 156.34.222.13 80
PROXY ABC 47.29.201.179 5316 156.34.222.13 80
Non-successful
Send PROXY probe
200 OK
Send malformed PROXY probe
Non-successful
Regular bypass
200 OK
False positive
GET /
Send regular probe
200 OK
Discard

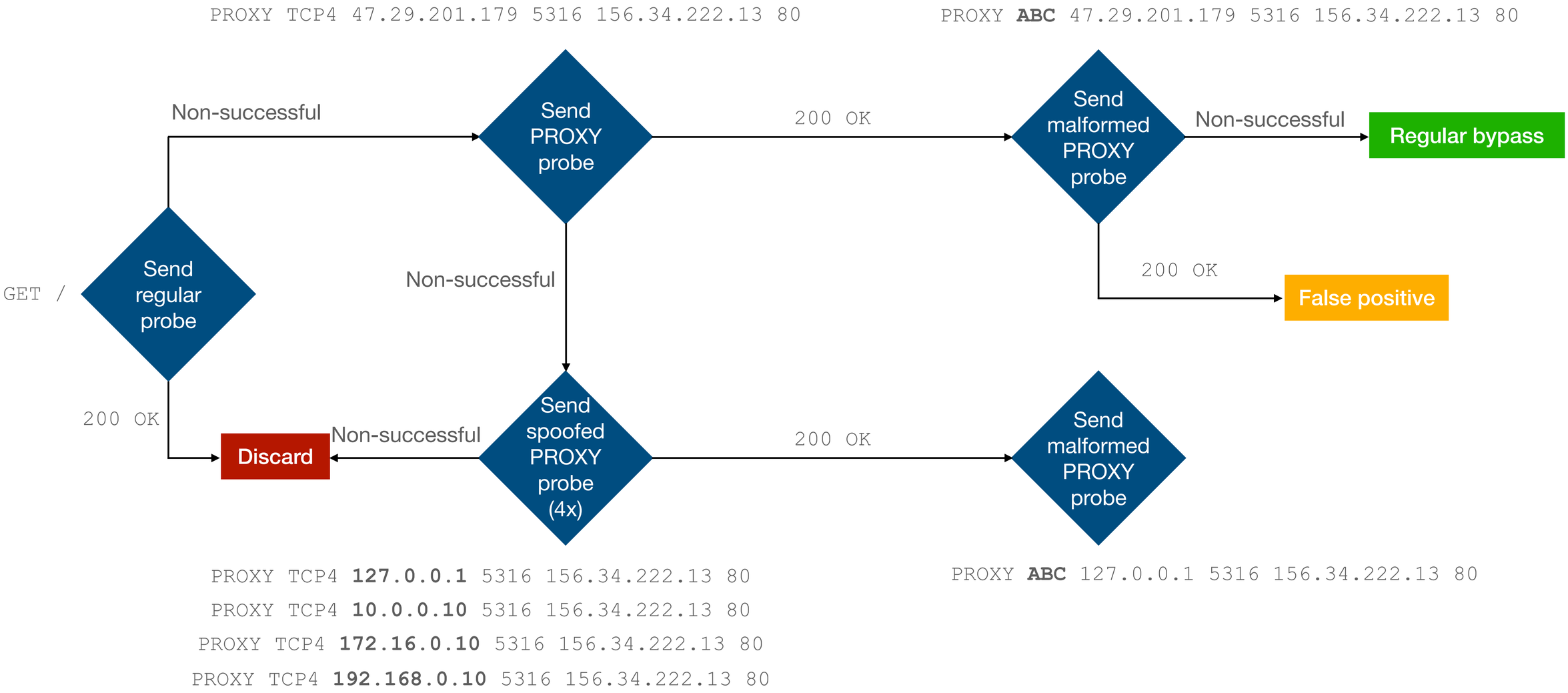
Our Method


PROXY TCP4 47.29.201.179 5316 156.34.222.13 80
PROXY ABC 47.29.201.179 5316 156.34.222.13 80
Non-successful
Send PROXY probe
200 OK
Send malformed PROXY probe
Non-successful
Regular bypass
200 OK
False positive
GET /
Send regular probe
Non-successful
200 OK
Discard
Send spoofed PROXY probe (4x)

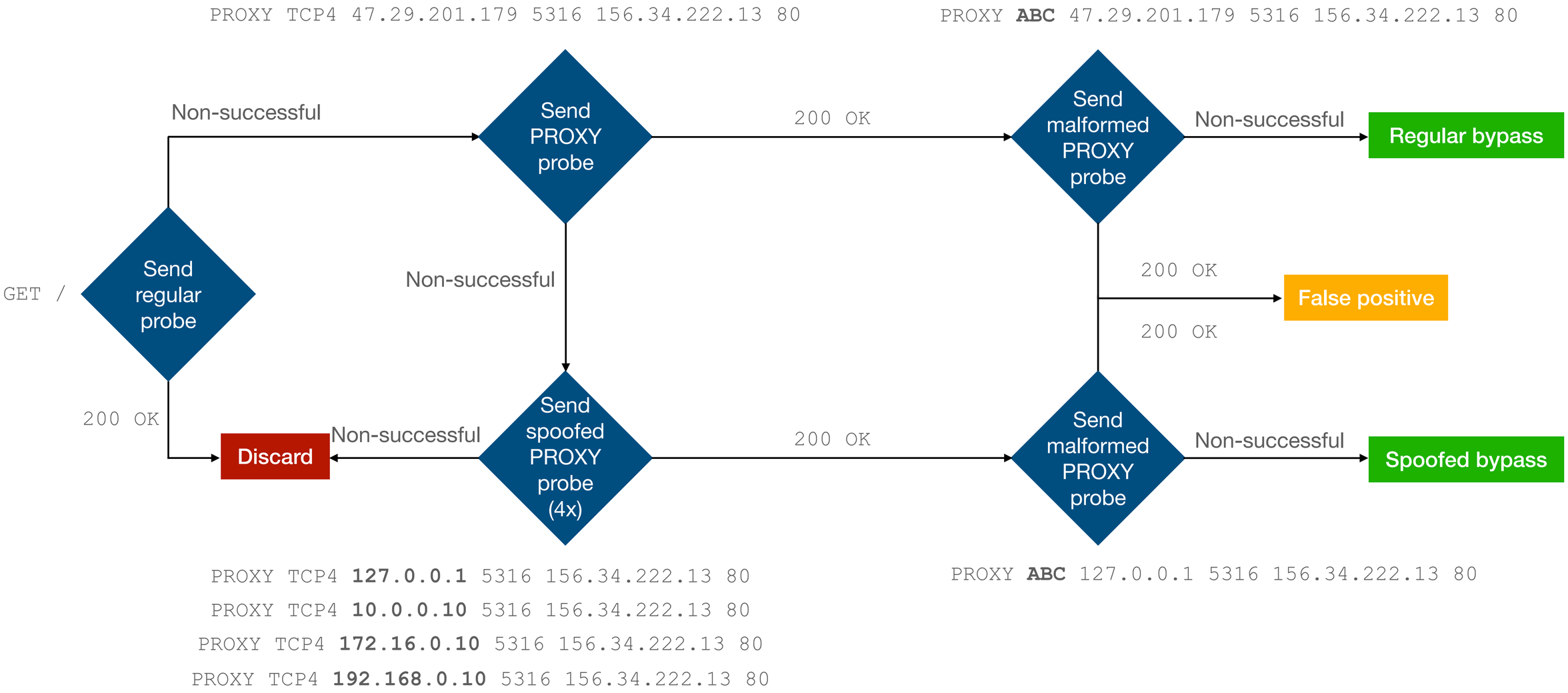
Our Method


PROXY TCP4 47.29.201.179 5316 156.34.222.13 80
PROXY ABC 47.29.201.179 5316 156.34.222.13 80
Non-successful
Send PROXY probe
200 OK
Send malformed PROXY probe
Non-successful
Regular bypass
200 OK
False positive
GET /
Send regular probe
Non-successful
200 OK
Discard
Send spoofed PROXY probe (4x)
PROXY TCP4 127.0.0.1 5316 156.34.222.13 80
PROXY TCP4 10.0.0.10 5316 156.34.222.13 80
PROXY TCP4 172.16.0.10 5316 156.34.222.13 80
PROXY TCP4 192.168.0.10 5316 156.34.222.13 80

Our Method


PROXY TCP4 47.29.201.179 5316 156.34.222.13 80
PROXY ABC 47.29.201.179 5316 156.34.222.13 80
Non-successful
Send PROXY probe
200 OK
Send malformed PROXY probe
Non-successful
Regular bypass
200 OK
False positive
GET /
Send regular probe
Non-successful
200 OK
Discard
Non-successful
Send spoofed PROXY probe (4x)
200 OK
Send malformed PROXY probe
PROXY TCP4 127.0.0.1 5316 156.34.222.13 80
PROXY TCP4 10.0.0.10 5316 156.34.222.13 80
PROXY TCP4 172.16.0.10 5316 156.34.222.13 80
PROXY TCP4 192.168.0.10 5316 156.34.222.13 80
PROXY ABC 127.0.0.1 5316 156.34.222.13 80

Our Method


PROXY TCP4 47.29.201.179 5316 156.34.222.13 80
PROXY ABC 47.29.201.179 5316 156.34.222.13 80
Send regular probe
GET /
Non-successful
Send PROXY probe
200 OK
Send malformed PROXY probe
Non-successful
Regular bypass
200 OK
False positive
200 OK
Non-successful
Send spoofed PROXY probe (4x)
200 OK
Send malformed PROXY probe
Non-successful
Spoofed bypass
200 OK
Discard
PROXY TCP4 127.0.0.1 5316 156.34.222.13 80
PROXY TCP4 10.0.0.10 5316 156.34.222.13 80
PROXY TCP4 172.16.0.10 5316 156.34.222.13 80
PROXY TCP4 192.168.0.10 5316 156.34.222.13 80
PROXY ABC 127.0.0.1 5316 156.34.222.13 80

Our Results

Large number of hosts accept PROXY headers from unknown sources

- 177,983 over HTTP
- 2,332,377 over SMTP
- 2,343,420 over SSH

Our Results

Large number of hosts accept PROXY headers from unknown sources

- 177,983 over HTTP
- 2,332,377 over SMTP
- 2,343,420 over SSH

PROXY header injection can bypass access controls

Analysis of 177,983 Web Pages

	Experiment Group	Control Group
Boilerplate	118,641 (66.66%)	64,544 (36.83%)
Login	34,474 (19.37%)	12,136 (6.82%)
Miscellaneous	12,791 (7.19%)	75,897 (42.64%)
Enable JavaScript	6,577 (3.70%)	1,439 (0.81%)
Cannot parse	3,697 (2.08%)	3,696 (2.08%)
NGINX	1,345 (0.76%)	12,875 (7.23%)
Temperature Measurement	304 (0.17%)	6 (<0.01%)
Construction	107 (0.06%)	507 (0.28%)
Apache	47 (0.03%)	6,883 (3.87%)

Analysis of 177,983 Web Pages

	Experiment Group	Control Group
Boilerplate	118,641 (66.66%)	64,544 (36.83%)
Login	34,474 (19.37%)	12,136 (6.82%)
Miscellaneous	12,791 (7.19%)	75,897 (42.64%)
Enable JavaScript	6,577 (3.70%)	1,439 (0.81%)
Cannot parse	3,697 (2.08%)	3,696 (2.08%)
NGINX	1,345 (0.76%)	12,875 (7.23%)
Temperature Measurement	304 (0.17%)	6 (<0.01%)
Construction	107 (0.06%)	507 (0.28%)
Apache	47 (0.03%)	6,883 (3.87%)

Analysis of 177,983 Web Pages

	Experiment Group	Control Group
Boilerplate	118,641 (66.66%)	64,544 (36.83%)
Login	34,474 (19.37%)	12,136 (6.82%)
Miscellaneous	12,791 (7.19%)	75,897 (42.64%)
Enable JavaScript	6,577 (3.70%)	1,439 (0.81%)
Cannot parse	3,697 (2.08%)	3,696 (2.08%)
NGINX	1,345 (0.76%)	12,875 (7.23%)
Temperature Measurement	304 (0.17%)	6 (<0.01%)
Construction	107 (0.06%)	507 (0.28%)
Apache	47 (0.03%)	6,883 (3.87%)

Control: common web pages such as company websites, product advertisements, event information, personal websites, and educational institutions.

Analysis of 177,983 Web Pages

	Experiment Group	Control Group
Boilerplate	118,641 (66.66%)	64,544 (36.83%)
Login	34,474 (19.37%)	12,136 (6.82%)
Miscellaneous	12,791 (7.19%)	75,897 (42.64%)
Enable JavaScript	6,577 (3.70%)	1,439 (0.81%)
Cannot parse	3,697 (2.08%)	3,696 (2.08%)
NGINX	1,345 (0.76%)	12,875 (7.23%)
Temperature Measurement	304 (0.17%)	6 (<0.01%)
Construction	107 (0.06%)	507 (0.28%)
Apache	47 (0.03%)	6,883 (3.87%)

Control: common web pages such as company websites, product advertisements, event information, personal websites, and educational institutions.

Experiment: 36% provide an access portal to **home automation systems**, temperature sensors, electric vehicle charging station **diagnostics**, Internet of Things (IoT) sensors, and **intrusion alarm monitoring**,

Analysis of 177,983 Web Pages

	Experiment Group	Control Group
Boilerplate	118,641 (66.66%)	64,544 (36.83%)
Login	34,474 (19.37%)	12,136 (6.82%)
Miscellaneous	12,791 (7.19%)	75,897 (42.64%)
Enable JavaScript	6,577 (3.70%)	1,439 (0.81%)
Cannot parse	3,697 (2.08%)	3,696 (2.08%)
NGINX	1,345 (0.76%)	12,875 (7.23%)
Temperature Measurement	304 (0.17%)	6 (<0.01%)
Construction	107 (0.06%)	507 (0.28%)
Apache	47 (0.03%)	6,883 (3.87%)

Control: common web pages such as company websites, product advertisements, event information, personal websites, and educational institutions.

Experiment: 36% provide an access portal to **home automation systems**, temperature sensors, electric vehicle charging station **diagnostics**, Internet of Things (IoT) sensors, and **intrusion alarm monitoring**,

Could potentially extend to over 4,600 pages!

Spoofed Bypasses

Header \ No Header	Unsuccessful	4xx	403
2xx Non-internal IP	5,863 (11,640)	648 (3,430)	211 (953)
2xx 127.0.0.1	6,609 (12,235)	1,041 (3,773)	252 (978)
2xx 10.0.0.10	7,480 (13,107)	1,029 (3,762)	246 (974)
2xx 172.16.0.10	7,660 (13,313)	1,011 (3,754)	235 (961)
2xx 192.168.0.10	5,899 (11,527)	1,027 (3,766)	239 (967)

Our Results

Large number of hosts accept PROXY headers from unknown sources

- 177,983 over HTTP
- 2,332,377 over SMTP
- 2,343,420 over SSH

PROXY header injection can bypass access controls

Including to:
- Private dashboards
- Home automation devices
- IoT monitoring services

Potentially over 4,000 affected websites

Our Results

Large number of hosts accept PROXY headers from unknown sources

- 177,983 over HTTP
- 2,332,377 over SMTP
- 2,343,420 over SSH

PROXY header injection can bypass access controls

Including to:
- Private dashboards
- Home automation devices
- IoT monitoring services

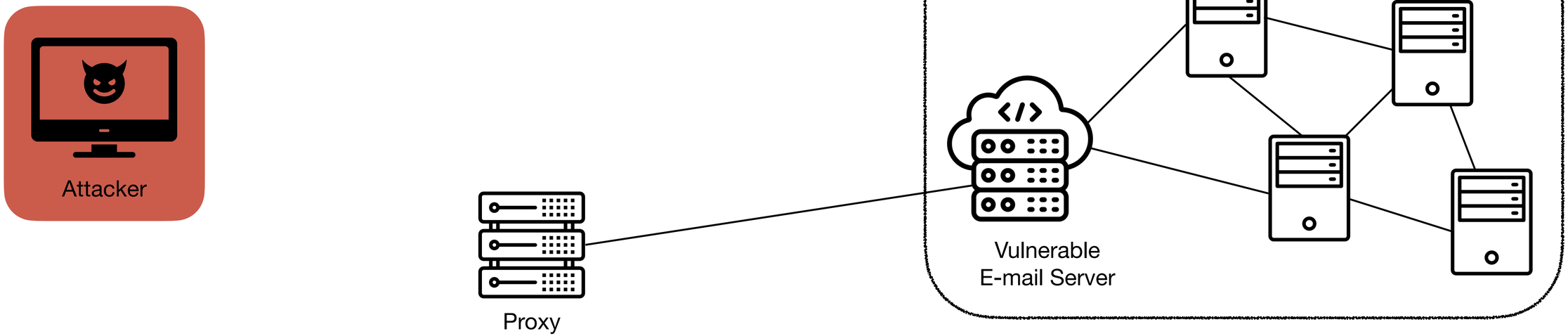
Potentially over 4,000 affected websites

PROXY header injection can turn SMTP servers into open relays

SMTP Example: Postfix

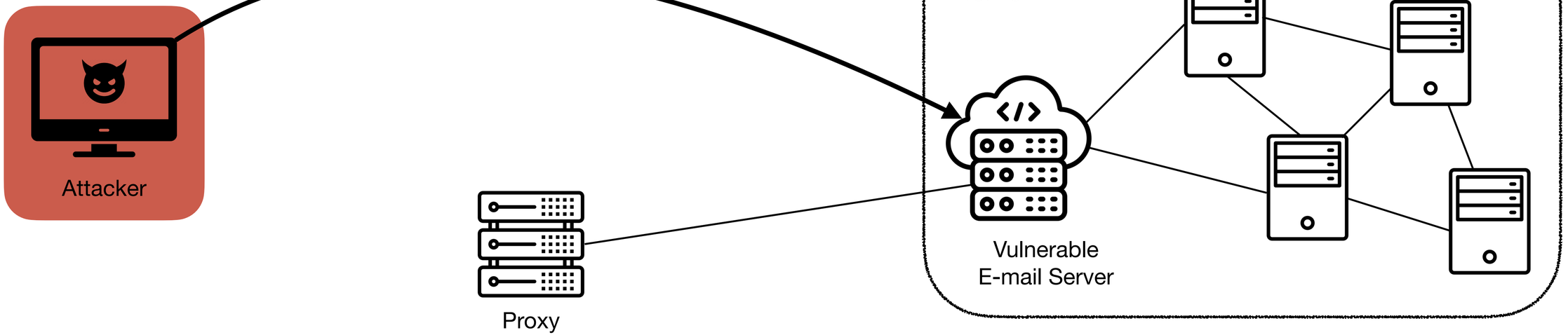
- By default, Postfix only relays emails coming from the `localhost` address
- To bypass this, an attacker needs to “convince” the Postfix server that the email originates from the `localhost` address
  - We can use the PROXY protocol for this! (Spoofed bypass)

Example

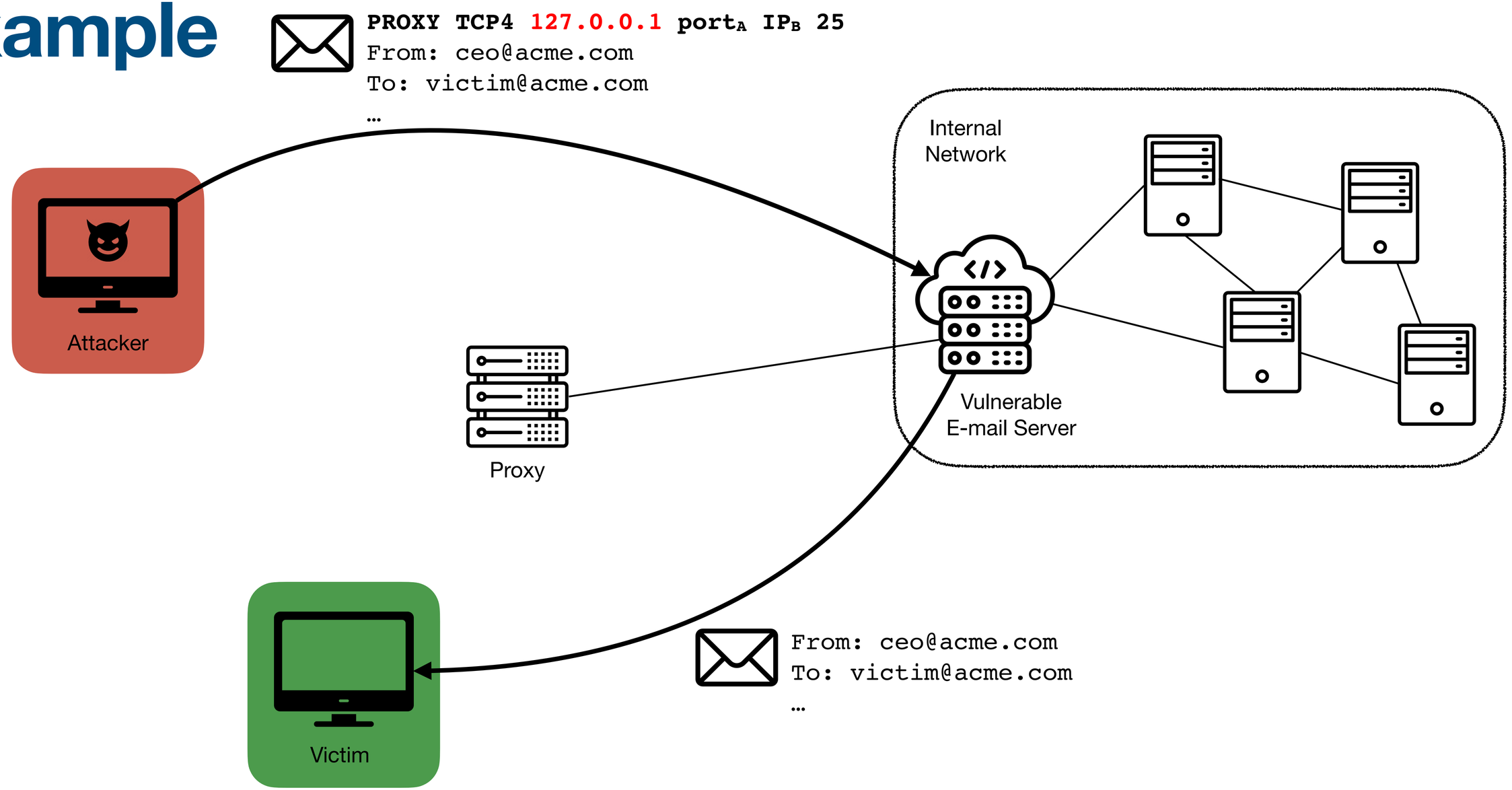

Attacker
Proxy
Internal
Network
Vulnerable
E-mail Server
Victim

Example

```
PROXY TCP4 127.0.0.1 portA IPB 25
From: ceo@acme.com
To: victim@acme.com
…
```



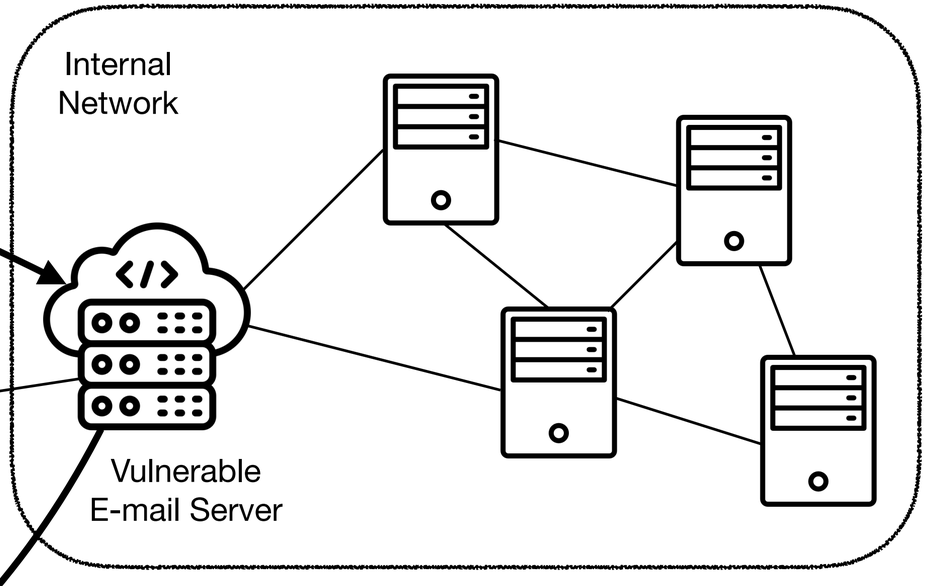
Example


PROXY TCP4 127.0.0.1 portA IPB 25
From: ceo@acme.com
To: victim@acme.com
…
Internal
Network
Attacker
Proxy
Vulnerable
E-mail Server
Victim
From: ceo@acme.com
To: victim@acme.com
…

Example

```
PROXY TCP4 127.0.0.1 portA IPB 25
From: ceo@acme.com
To: victim@acme.com
…
```

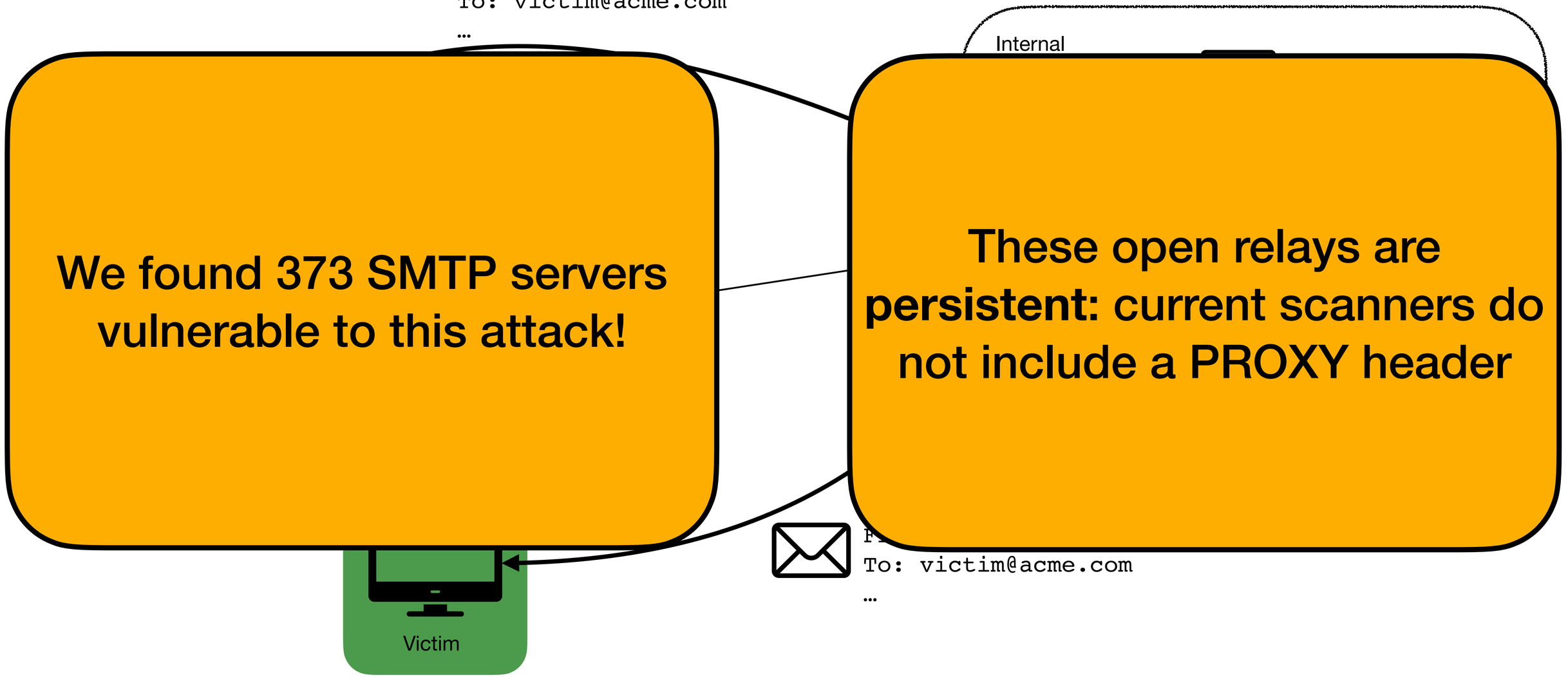
We found 373 SMTP servers vulnerable to this attack!



```
From: ceo@acme.com
To: victim@acme.com
…
```

Example

```
PROXY TCP4 127.0.0.1 portA IPB 25
From: ceo@acme.com
To: victim@acme.com
…
```



Our Results

Large number of hosts accept PROXY headers from unknown sources

- 177,983 over HTTP
- 2,332,377 over SMTP
- 2,343,420 over SSH

PROXY header injection can bypass access controls

Including to:
- Private dashboards
- Home automation devices
- IoT monitoring services

Potentially over 4,000 affected websites

PROXY header injection can turn SMTP servers into open relays

- Impersonate any email address
- Undetectable by current scanners
- At least 373 vulnerable email servers

Ethics

- All scans contained opt-out mechanisms
- We used a `HEAD` request for the spoofed probes to avoid leaking sensitive information
- All emails were sent from and to addresses under our control
- All affected parties were notified through responsible disclosure
  - Yes, we received bounties

Summary

- First study on the prevalence and security implications of the PROXY protocol

- Many backend servers will happily accept unsolicited PROXY headers from unknown clients

- This can lead to severe security implications:
  - Exposes internal networks
  - Gives access to private information and control systems
  - Turns SMTP servers into open relays

Summary

- First study on the prevalence and security implications of the PROXY protocol

- Many backend servers will happily accept unsolicited PROXY headers from unknown clients

- This can lead to severe security implications:
  - Exposes internal networks
  - Gives access to private information and control systems
  - Turns SMTP servers into open relays

Thank You! Questions?

Stijn Pletinckx, Christopher Kruegel, Giovanni Vigna

stijn@ucsb.edu

University of California, Santa Barbara