Connecting DDoS protection: things to consider

Ramil Khantimirov, Ph.D.

CEO StormWall

10 February 2017

I stopped service

Bcz attacker targeted us and attack on ptp ip

That provider couldn't protect itself

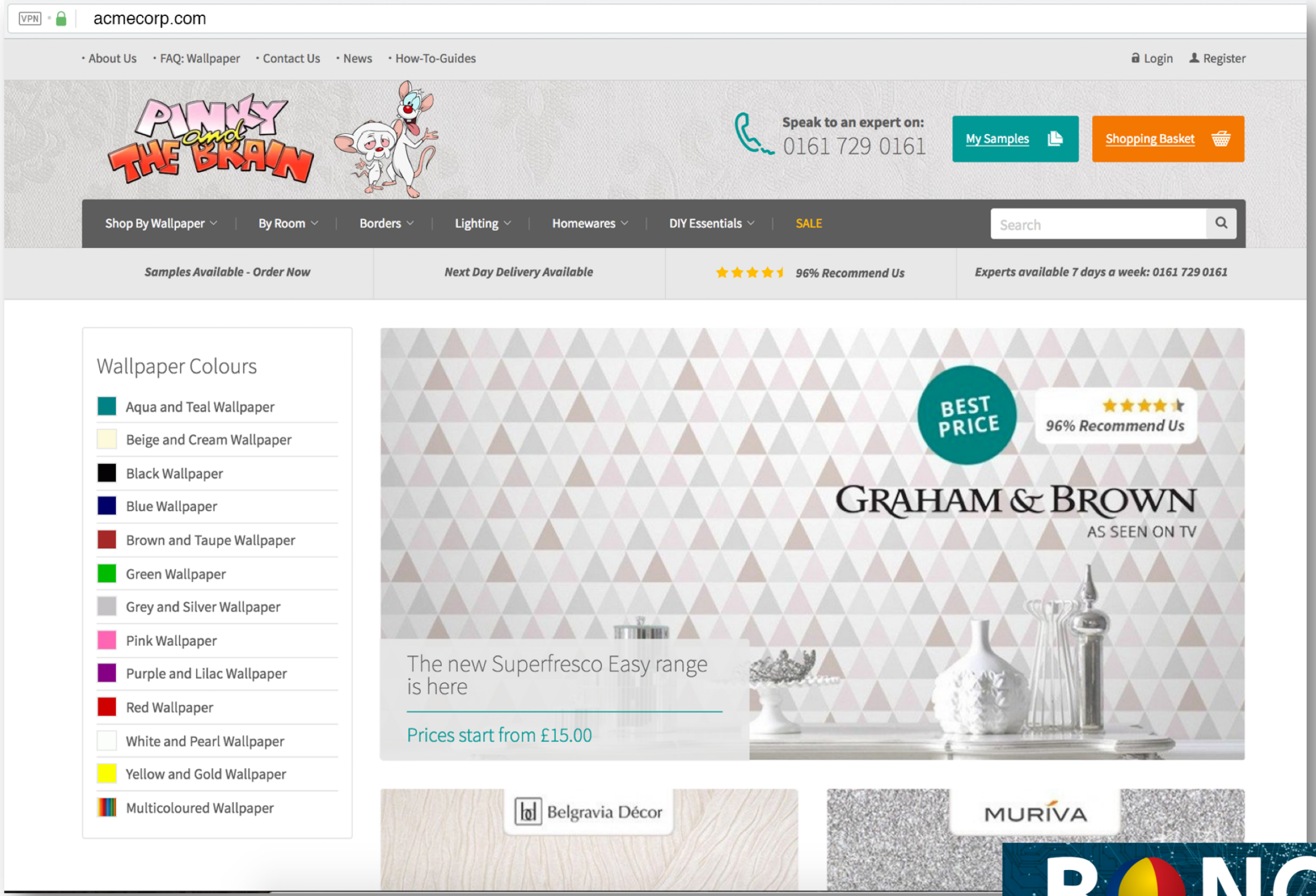
I stopped selling bandwidth

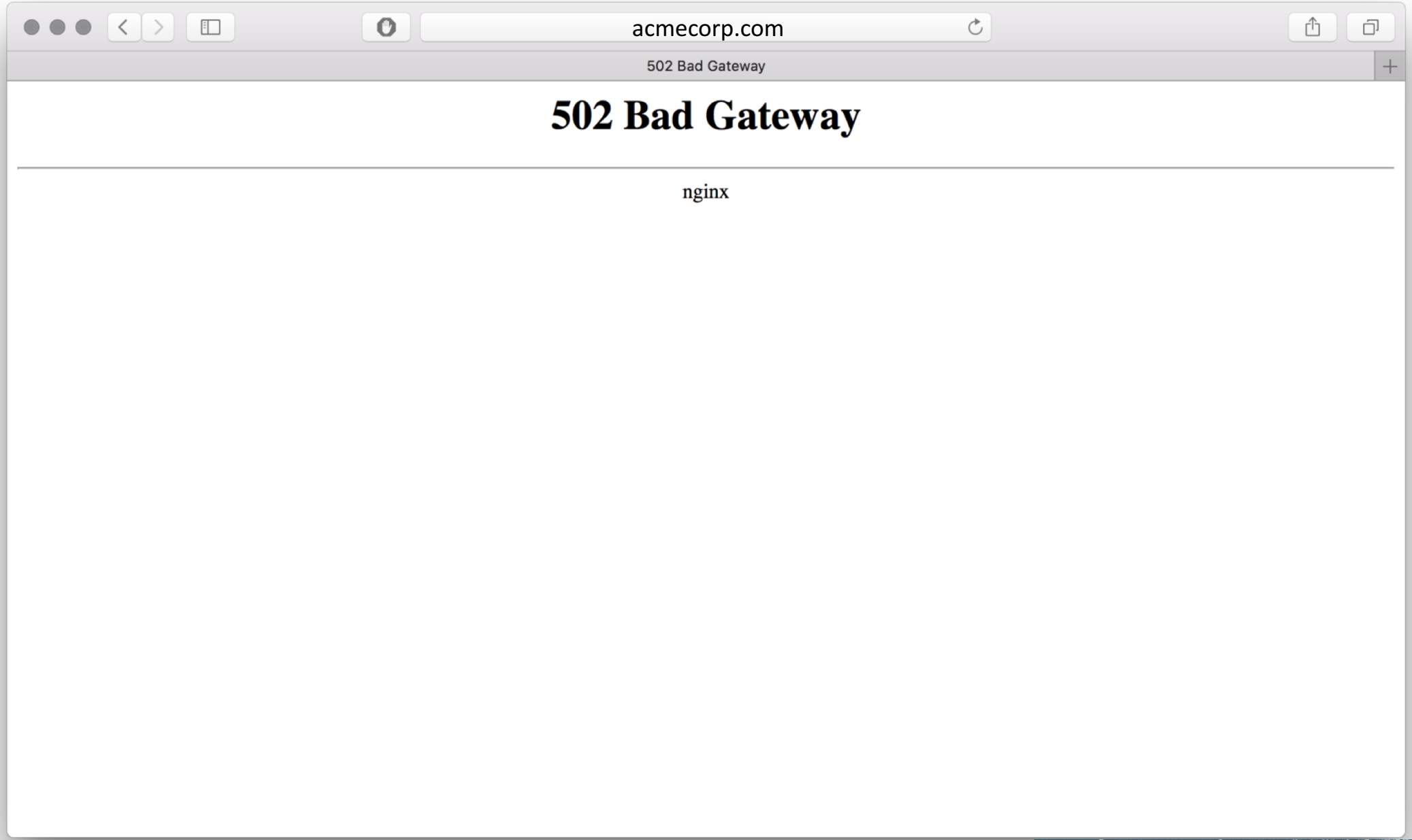
I had no choice

CERTIFICATE OF INCORPORATION

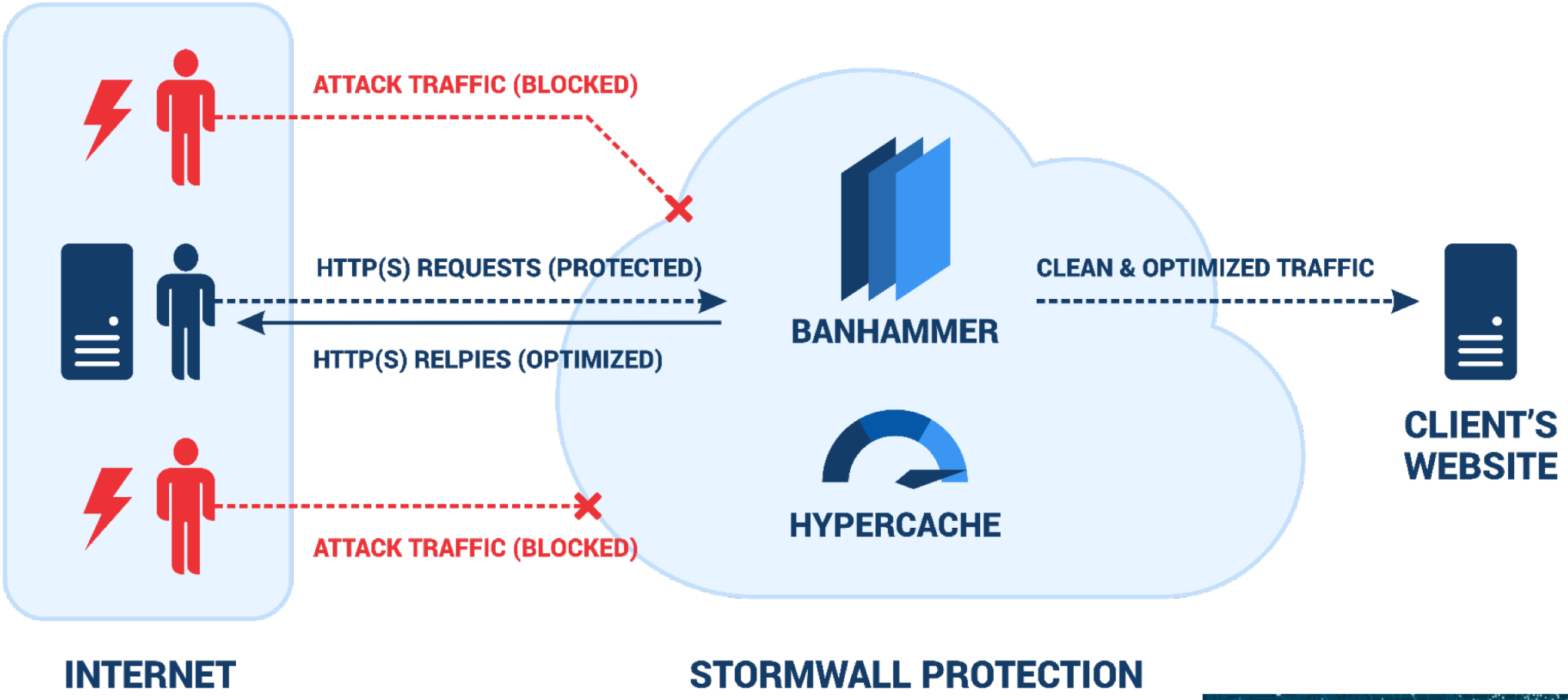
OF A PRIVATE LIMITED COMPANY

Company No. 3300636


acmecorp.com
About Us
FAQ: Wallpaper
Contact Us
News
How-To-Guides
Login
Register
Pinky and The Brain
Speak to an expert on:
0161 729 0161
My Samples
Shopping Basket
Shop By Wallpaper
By Room
Borders
Lighting
Homewares
DIY Essentials
SALE
Search
Samples Available - Order Now
Next Day Delivery Available
96% Recommend Us
Experts available 7 days a week: 0161 729 0161
Wallpaper Colours
Aqua and Teal Wallpaper
Beige and Cream Wallpaper
Black Wallpaper
Blue Wallpaper
Brown and Taupe Wallpaper
Green Wallpaper
Grey and Silver Wallpaper
Pink Wallpaper
Purple and Lilac Wallpaper
Red Wallpaper
White and Pearl Wallpaper
Yellow and Gold Wallpaper
Multicoloured Wallpaper
BEST PRICE
96% Recommend Us
GRAHAM & BROWN
AS SEEN ON TV
The new Superfresco Easy range is here
Prices start from £15.00
Belgravia Décor
MURIVA


acmecorp.com
502 Bad Gateway
502 Bad Gateway
nginx

How website protection is connected?



Whois Web Hosting Information for website – acmecorp.com –

29 October 2017, 16:58:40

Hosting Info for Website:	**acmecorp.com**
Popularity:	3,160 visitors per day
IP Address:	22.22.22.22
IP Location:	USA, Pennsylvania, Wayne
IP Reverse DNS (Host):	u18241529.onlinehome-server.com
Whois Record Created:	22 Nov 2006
Whois Record Updated:	09 Aug 2017
IP Address Change History:	**Acmecorp.com Website used IP Addresses -** 11.11.11.11 (64.73.195.38) used on 20 December 2015 • 97.74.34.228 • 74.208.123.1 More Information

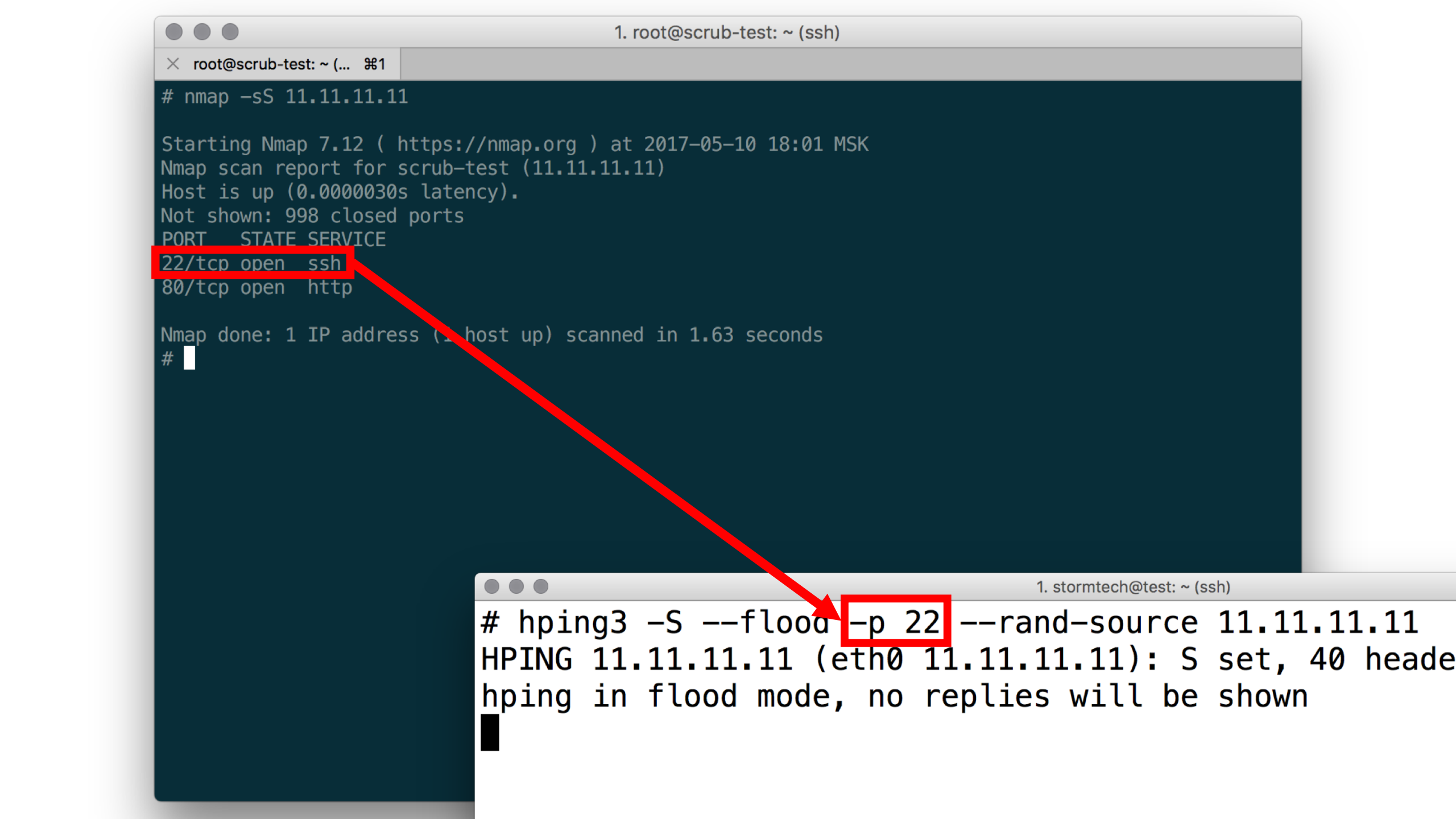
#275,322 position in world sites rating

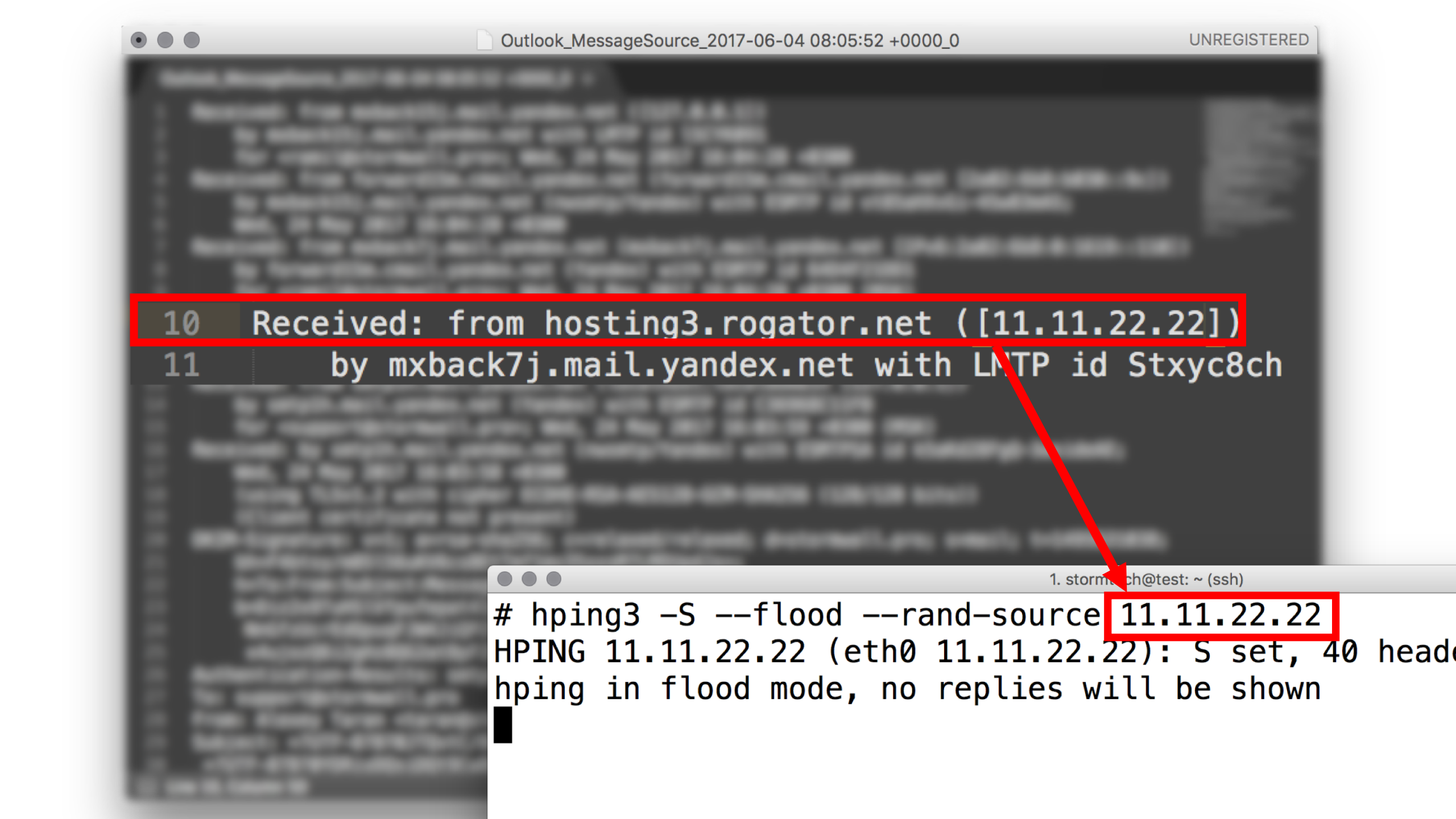
Hide Map »

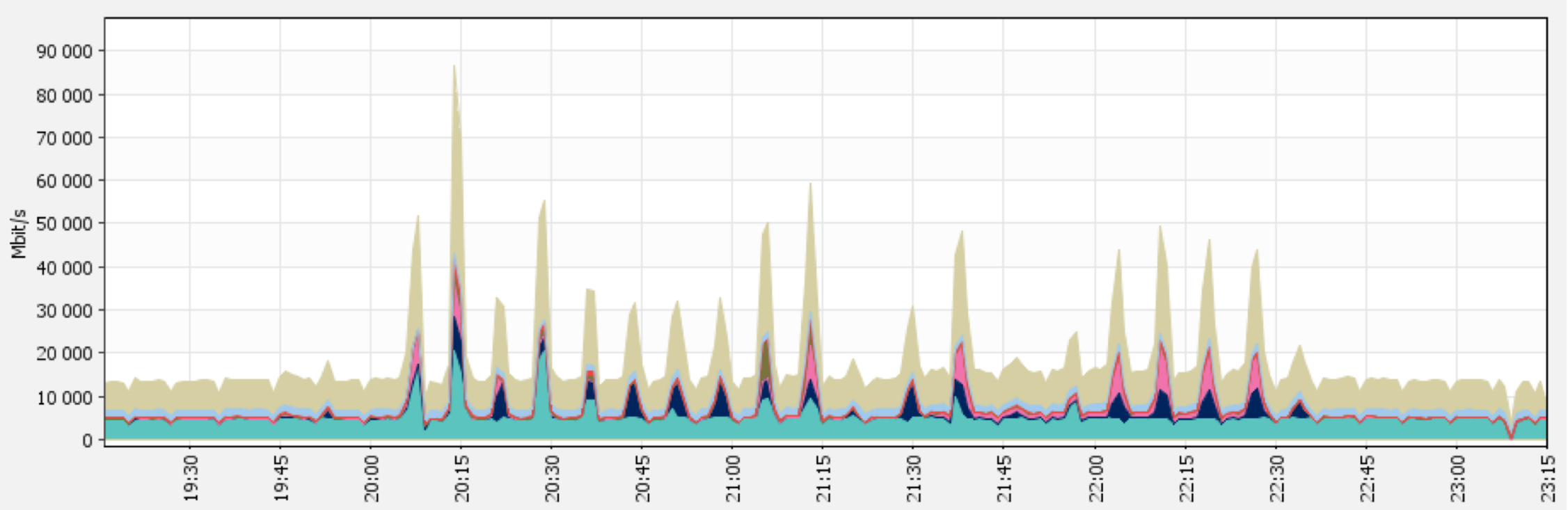
Website Review »

API Example - Export to Text File

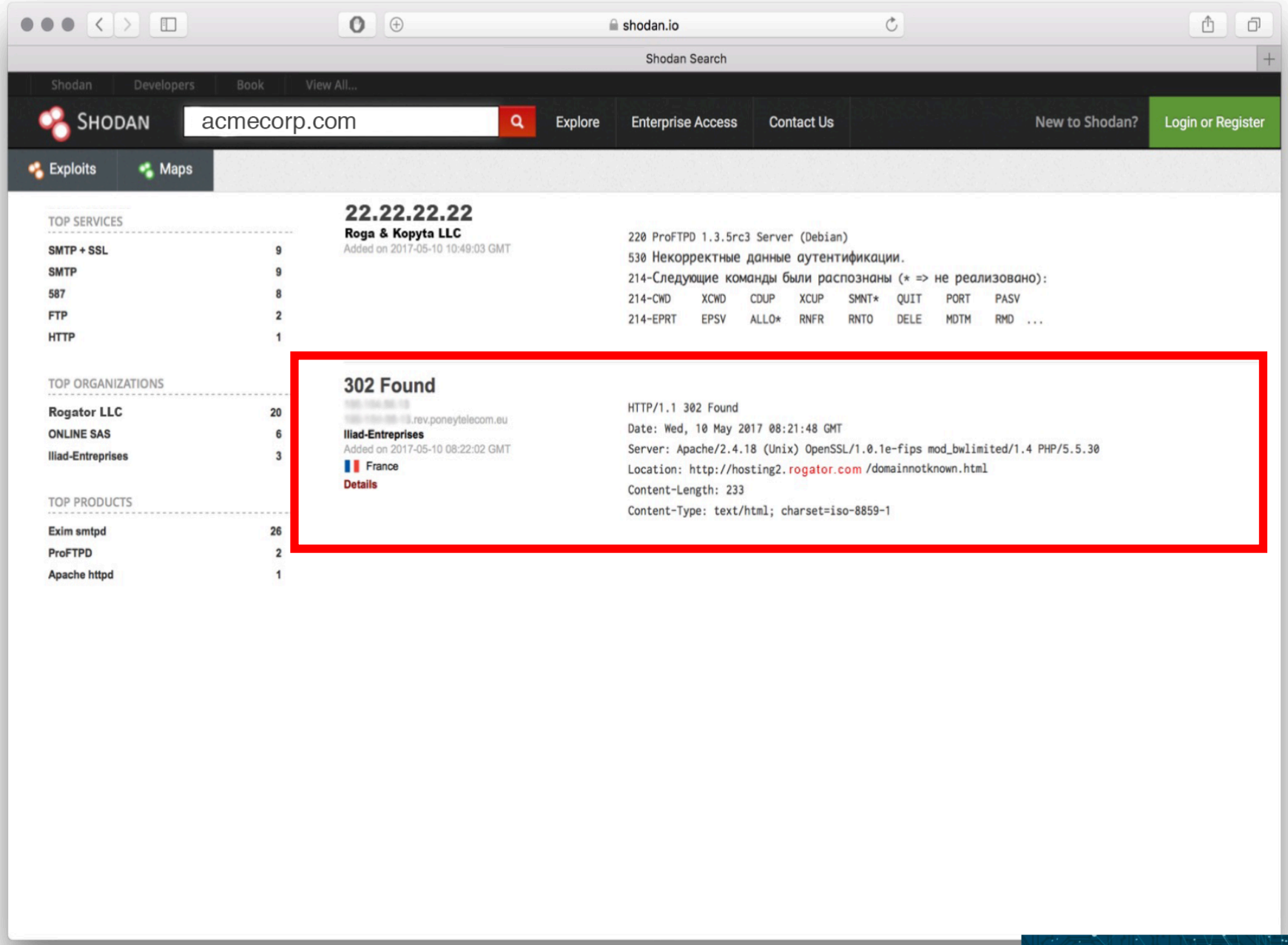
```
1. stormtech@test: ~ (ssh)
# hping3 -S --flood --rand-source 11.11.11.11
HPING 11.11.11.11 (eth0 11.11.11.11): S set, 40
hping in flood mode, no replies will be shown
```


1. root@scrub-test: ~ (ssh)
root@scrub-test: ~ (... ⌘1
nmap -sS 11.11.11.11
Starting Nmap 7.12 (https://nmap.org) at 2017-05-10 18:01 MSK
Nmap scan report for scrub-test (11.11.11.11)
Host is up (0.0000030s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
#
1. stormtech@test: ~ (ssh)
hping3 -S --flood -p 22 --rand-source 11.11.11.11
HPING 11.11.11.11 (eth0 11.11.11.11): S set, 40 heade
hping in flood mode, no replies will be shown


Outlook_MessageSource_2017-06-04 08:05:52 +0000_0
UNREGISTERED
10 Received: from hosting3.rogator.net ([11.11.22.22])
11 by mxback7j.mail.yandex.net with LMTP id Stxyc8ch
1. stormech@test: ~ (ssh)
hping3 -S --flood --rand-source 11.11.22.22
HPING 11.11.22.22 (eth0 11.11.22.22): S set, 40 head
hping in flood mode, no replies will be shown


Mbit/s
90 000
80 000
70 000
60 000
50 000
40 000
30 000
20 000
10 000
0
19:30
19:45
20:00
20:15
20:30
20:45
21:00
21:15
21:30
21:45
22:00
22:15
22:30
22:45
23:00
23:15

RONOG 4


shodan.io
Shodan Search
Shodan
Developers
Book
View All...
SHODAN
acmecorp.com
Explore
Enterprise Access
Contact Us
New to Shodan?
Login or Register
Exploits
Maps
TOP SERVICES
SMTP + SSL 9
SMTP 9
587 8
FTP 2
HTTP 1
TOP ORGANIZATIONS
Rogator LLC 20
ONLINE SAS 6
Iliad-Entreprises 3
TOP PRODUCTS
Exim smtpd 26
ProFTPD 2
Apache httpd 1
22.22.22.22
Roga & Kopyta LLC
Added on 2017-05-10 10:49:03 GMT
220 ProFTPD 1.3.5rc3 Server (Debian)
530 Некорректные данные аутентификации.
214-Следующие команды были распознаны (* => не реализовано):
214-CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV
214-EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD ...
302 Found
.rev.poneytelecom.eu
Iliad-Entreprises
Added on 2017-05-10 08:22:02 GMT
France
Details
HTTP/1.1 302 Found
Date: Wed, 10 May 2017 08:21:48 GMT
Server: Apache/2.4.18 (Unix) OpenSSL/1.0.1e-fips mod_bwlimited/1.4 PHP/5.5.30
Location: http://hosting2.rogator.com /domainnotknown.html
Content-Length: 233
Content-Type: text/html; charset=iso-8859-1

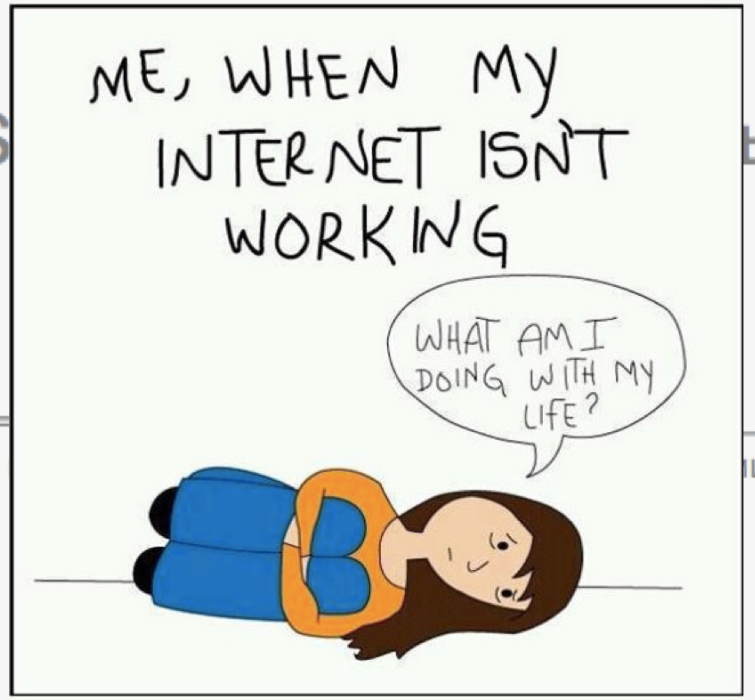
Tips: protecting website from DDoS

- New IP address, access only from DDoS protection IP
- Change hosting (if possible)
- Separate SMTP server

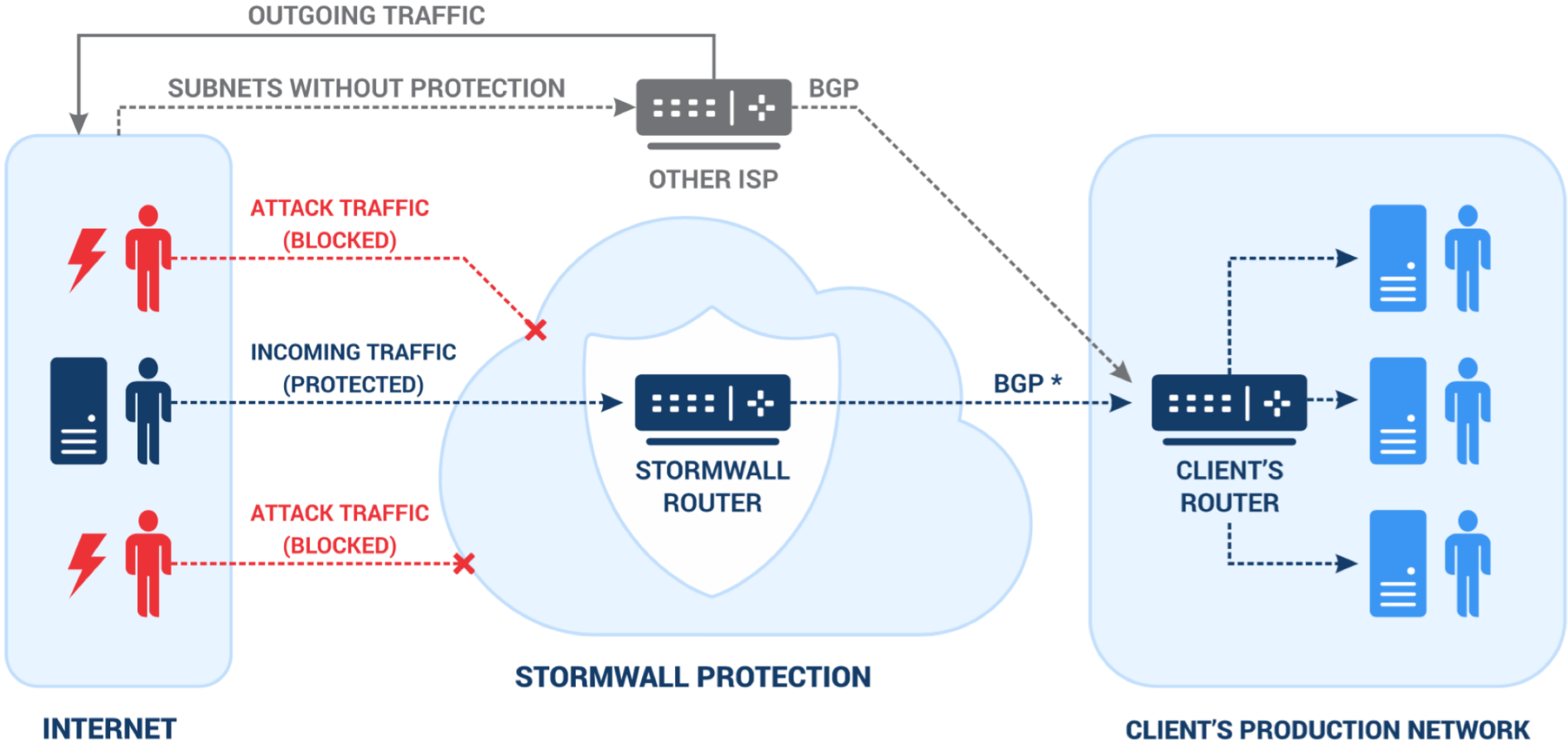
TELECOM

RONOG 4

google.ru

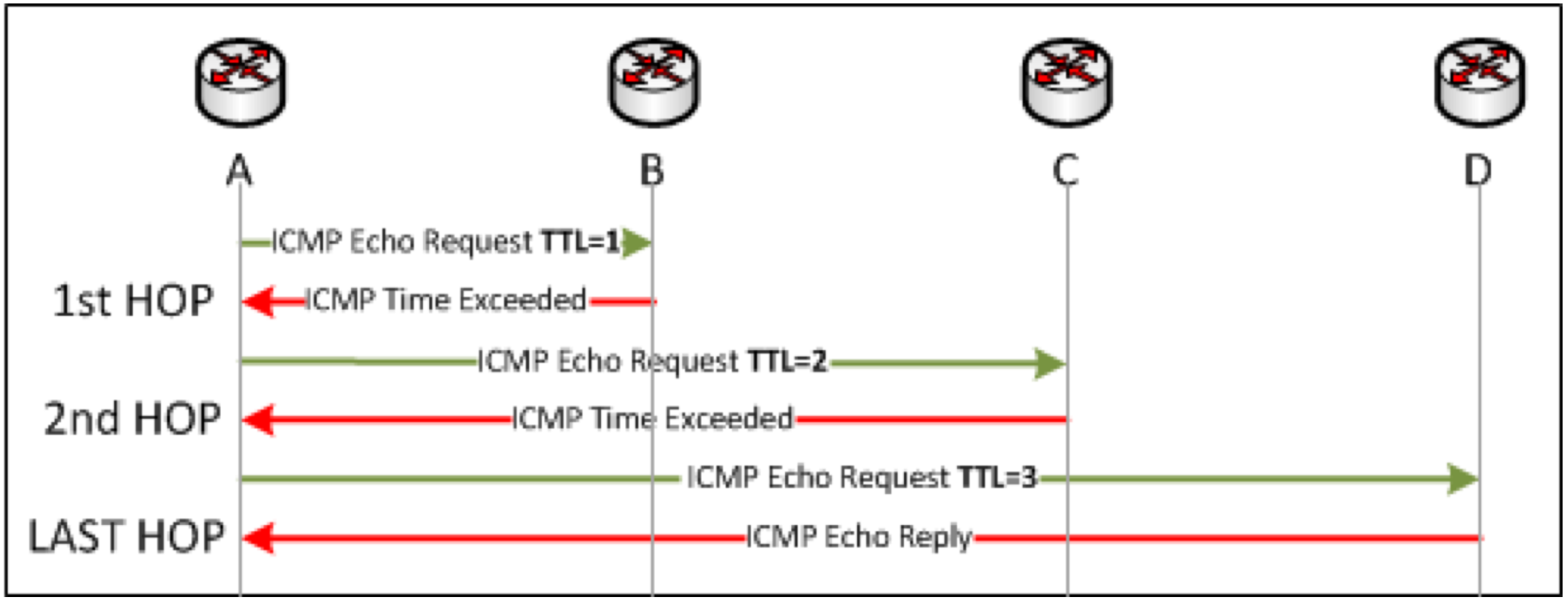


How network protection is connected?



*Over IPIP / GRE tunnel or direct connection

How traceroute works?



```
# mtr --report-cycles=10 --report 4.4.4.4
Start: Fri Jun  2 12:53:24 2017
HOST: MacBook-Pro.local                Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 14.12.24.1                      0.0%    10   47.5  47.6  47.0  49.5   0.6
  2.|-- 100.7.1.1                       0.0%    10   47.3  47.6  47.1  48.8   0.0
  3.|-- 14.12.24.147                    10.0%    10  513.5 506.7 477.5 561.6  23.7
  4.|-- 195.229.69.201                   0.0%    10   85.4  84.7  84.1  86.7   0.7
  5.|-- if-ae-14-3.tcore2.fnm-fra 10.0%    10  101.4 106.0 101.4 120.8   7.3
  6.|-- anti-ddos-service                0.0%    10  101.3 101.9 101.1 104.6   0.9
  7.|-- 3.3.3.3                          0.0%    10  147.0 147.9 146.1 151.0   1.2
  8.|-- 4.4.4.4                          0.0%    10  148.2 148.1 146.1 151.0   1.3
```

```
# mtr --report-cycles=10 --report 4.4.4.4
Start: Fri Jun  2 12:53:24 2017
HOST: MacBook-Pro.local                Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 14.12.24.1                      0.0%    10   47.5  47.6  47.0  49.5   0.6
  2.|-- 100.7.1.1                       0.0%    10   47.3  47.6  47.1  48.8   0.0
  3.|-- 14.12.24.147                    10.0%    10  513.5 506.7 477.5 561.6  23.7
  4.|-- 195.229.69.201                   0.0%    10   85.4  84.7  84.1  86.7   0.7
  5.|-- if-ae-14-3.tcore2.fnm-fra       10.0%    10  101.4 106.0 101.4 120.8   7.3
  6.|-- anti-ddos-service                0.0%    10  101.3 101.9 101.1 104.6   0.9
  7.|-- 3.3.3.3                         81.2%    10  764.0 654.9 146.1 932.0   530
  8.|-- 4.4.4.4                         100.0    10    0.0   0.0   0.0   0.0   0.0
```

How to hide IP address from traceroute?

1. You have a switch

ICMP drop:
- ttl expired
- port unreachable
- echo reply

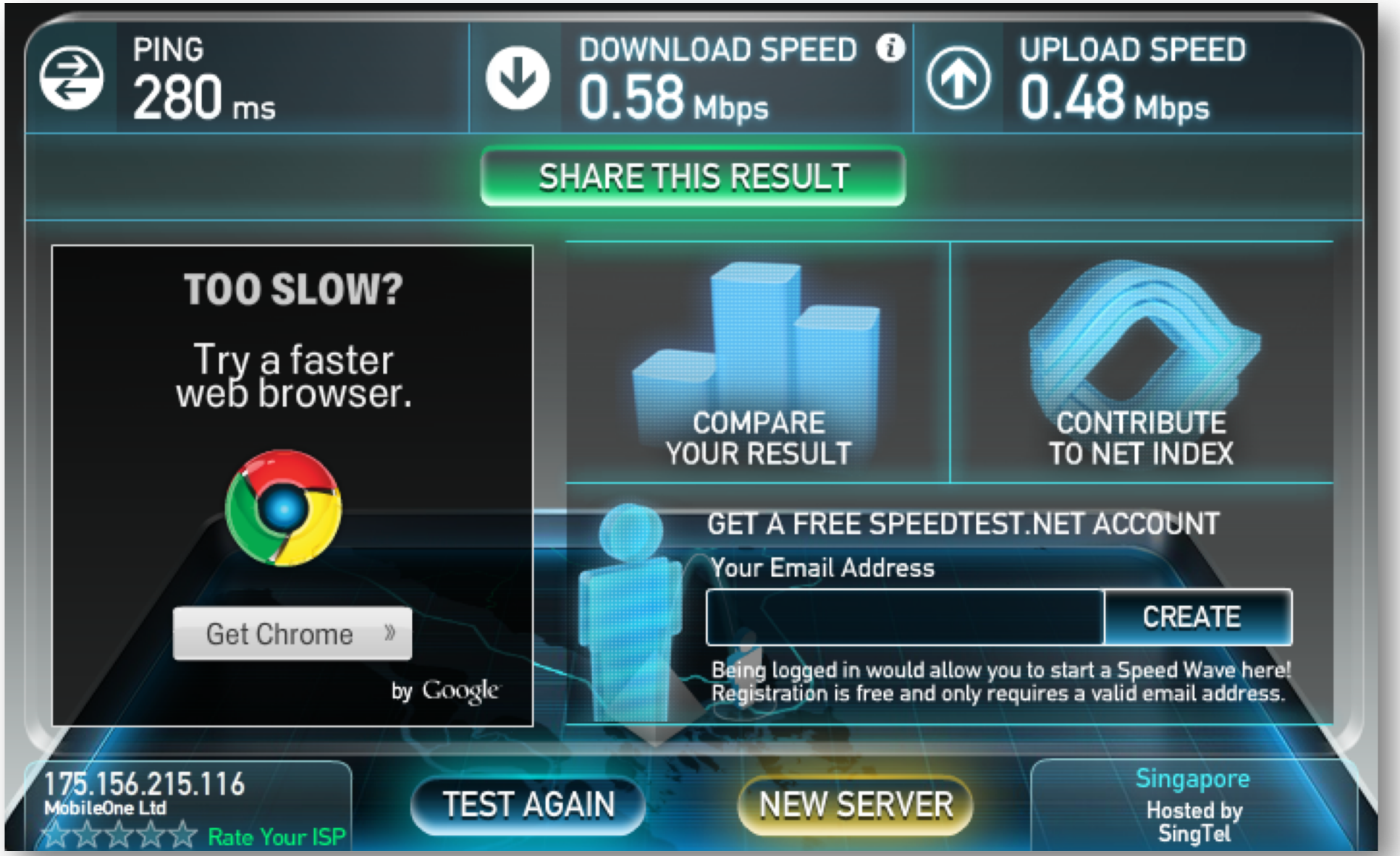
2. You don’t have a switch

2.1. Same as p.1 (good)

2.2. TTL+1

2.3. Drop all packets with TTL <=1

2.4. Drop ICMP + UDP ports 33434 to 33534 (bad idea!)


PING
280 ms
DOWNLOAD SPEED
0.58 Mbps
UPLOAD SPEED
0.48 Mbps
SHARE THIS RESULT
TOO SLOW?
Try a faster web browser.
Get Chrome
by Google
COMPARE YOUR RESULT
CONTRIBUTE TO NET INDEX
GET A FREE SPEEDTEST.NET ACCOUNT
Your Email Address
CREATE
Being logged in would allow you to start a Speed Wave here!
Registration is free and only requires a valid email address.
175.156.215.116
MobileOne Ltd
Rate Your ISP
TEST AGAIN
NEW SERVER
Singapore
Hosted by
SingTel

RONOG 4

Tips: protecting a network from DDoS

- Hide peering IPs from traceroute
- Protect peering IPs
- Consider scanning from inside the network
- Choose DDoS protection with 24/7 support
- NAT or proxy – many IPs!
- Tell the protection company more details about the infrastructure

How the story ends?

Thank you for attention!

ramil@stormwall.pro

+7 (926) 700-00-11 (incl. whatsapp)

Telegram @ramilkh

Skype ramilkh