Testing DNS-over-TLS servers with the RIPE Atlas probes

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

First publication of this article on 18 July 2018

https://www.bortzmeyer.org/dns-over-tls-atlas-measures.html

The RIPE Atlas probes <https://atlas.ripe.net/> can now perform DNS-over-TLS measurements, following RFC 7858[1]. Several DNS-over-TLS servers exist. This article shows rapidly a few measurements.

To ask the RIPE Atlas probes <https://atlas.ripe.net/> to perform DNS-over-TLS tests, we will use the Blaeu software <https://labs.ripe.net/Members/stephane_bortzmeyer/creating-ripe-atlas Blaeu is made for one-off measurements, so the results here are not long-term measurements of the evolution of DNS-over-TLS servers. To do a DNS test with Blaeu, you use `blaeu-resolve` :

```
% blaeu-resolve mamot.fr
[2001:67c:288::14] : 5 occurrences
Test #15279055 done at 2018-07-18T21:06:14Z
```

By default, the Atlas probes will use the locally configured resolver. But we can direct the probes to a specific resolver, with `--nameserver` :

```
% blaeu-resolve --nameserver dns.quad9.net  www.france-ix.net
Nameserver dns.quad9.net
[2a00:a4c0:1:1::69] : 5 occurrences
Test #15279064 done at 2018-07-18T21:09:11Z
```

By default, this will use the usual DNS, in clear text, over UDP. But you can now ask for DNS over TLS, with `--tls` :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7858.txt`

```
% blaeu-resolve --nameserver dns.quad9.net  --tls www.bortzmeyer.org
Nameserver dns.quad9.net
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2605:4500:2:245b::42] : 5 occurrences
Test #15279068 done at 2018-07-18T21:10:29Z
```

The `--tls` option will instruct the Atlas probes to use TLS, here is the entire JSON request which has been sent :

```
% blaeu-resolve --nameserver dnsovertls.sinodun.com --verbose  --tls  signal.eu.org
{'is_oneoff': True, 'definitions': [{'description': 'DNS resolution of signal.eu.org/AAAA via nameserver dns
...
```

The `'tls': True` is the part that triggers DNS-over-TLS.

Now that we have this tool, what can we do? First, let's check if DNS-over-TLS works from everywhere. Some people voiced concerns that port 853, used by DNS-over-TLS, may be blocked on some networks. Let's try :

```
% blaeu-resolve --requested 1000 --nameserver getdnsapi.net --tls femen.org
Nameserver getdnsapi.net
[2607:5300:60:9fb5::2] : 126 occurrences
[TUCONNECT (may be a TLS negotiation error)] : 845 occurrences
[TIMEOUT] : 20 occurrences
Test #15279078 done at 2018-07-18T21:13:45Z
```

First problem, a lot of TLS negotiation errors. That's because most Atlas probes have old TLS code, and this specific server requires very recent TLS options and ciphers (we have the same problem with Cloudflare's `1.1.1.1` server and, indeed, with many servers). The probes are currently being upgraded but it is far from complete. Let's move to a server which is may be more lax :

```
% blaeu-resolve --requested 1000 --nameserver ns0.ldn-fai.net --tls femen.org
Nameserver ns0.ldn-fai.net
[TIMEOUT] : 970 occurrences
[TUCONNECT (may be a TLS negotiation error)] : 12 occurrences
[2607:5300:60:9fb5::2] : 10 occurrences
Test #15279106 done at 2018-07-18T21:21:59Z
```

OK, way too many timeouts. It could be because the small server cannot handle all the Atlas probes banging at the same time (Atlas has an option to add jitter but it is not used here). Let's try with another server :

```
% blaeu-resolve --requested 1000 --nameserver  unicast.censurfridns.dk  --tls  gitlab.isc.org
Nameserver unicast.censurfridns.dk
[2001:4f8:3:d::126] : 937 occurrences
[TIMEOUT] : 32 occurrences
[TUCONNECT (may be a TLS negotiation error)] : 12 occurrences
Test #15279169 done at 2018-07-18T21:42:11Z
```

OK, this is better, 3 % timeouts only. But it is still too much. Is it because of TLS? Let's try with regular DNS over TCP, without TLS, using the same set of probes (option `--old_measurement`) :

```
% blaeu-resolve --requested 1000 --old_measurement 15279169 --nameserver unicast.censurfridns.dk  --tcp  gitlab.
Warning: --requested=1000 ignored since a list of probes was requested
Nameserver unicast.censurfridns.dk
[2001:4f8:3:d::126] : 482 occurrences
[TUCONNECT (may be a TLS negotiation error)] : 6 occurrences
[TIMEOUT] : 5 occurrences
Test #15279208 done at 2018-07-18T21:51:15Z
```

This time, we have 1.0 % of timeouts, so it seems TLS has indeed problems. (The error message "may be a TLS negotiation error" is spurious <https://framagit.org/bortzmeyer/blaeu/issues/16>. The problems are instead connections refused by the server, or by a middlebox on the path.)

OK, may be the problem of timeouts is because the server `unicast.censurfridns.dk` is not well connected ? Let's try with a well managed and powerful server, Quad9 :

```
% blaeu-resolve --requested 1000 --nameserver 9.9.9.9 --tls www.ietf.org
Nameserver 9.9.9.9
[TIMEOUT] : 106 occurrences
[2400:cb00:2048:1::6814:155 2400:cb00:2048:1::6814:55] : 872 occurrences
[ERROR: SERVFAIL] : 1 occurrences
[TUCONNECT (may be a TLS negotiation error)] : 11 occurrences
Test #15277228 done at 2018-07-18T17:44:54Z
```

10 % of timeouts, that's certainly too much, and it proves that the 3 % problems before were not because the server was too weak. (Note there are also TLS negotiation errors, that shouldn't happen, but may have been triggered by middleboxes.) Again, let's try with ordinary DNS, using the same set of probes (unfortunately, many were not available for this comparison, so we have less results) :

```
% blaeu-resolve --nameserver 9.9.9.9 --old_measurement 15277228 www.ietf.org
Nameserver 9.9.9.9
[2400:cb00:2048:1::6814:155 2400:cb00:2048:1::6814:55] : 474 occurrences
[ERROR: SERVFAIL] : 2 occurrences
[TIMEOUT] : 19 occurrences
Test #15277243 done at 2018-07-18T17:53:42Z
```

Only 3.8 % of timeouts, that's better. So, it **seems** there is indeed a problem specific to port 853, but it seems quite server-specific. (A routing problem would have give the same results on port 53 and 853.) Remember to take these results with a serious grain of salt : it's one measurement, on a specific day and hour, and the Internet is always changing. Serious measurements would require doing it again at different times.

And, even when it works, is DNS-over-TLS much slower ? Let's display the RTT of the requests. First with TLS :

```
%  blaeu-resolve --nameserver dns.quad9.net --requested 1000 --tls --displayrtt  www.afnic.fr
Nameserver dns.quad9.net
[2001:67c:2218:30::24] : 849 occurrences Average RTT 2235 ms
[TIMEOUT] : 129 occurrences Average RTT 0 ms
[TUCONNECT (may be a TLS negotiation error)] : 15 occurrences Average RTT 0 ms
Test #15279140 done at 2018-07-18T21:34:30Z
```

Then with ordinary TCP :

```
%  blaeu-resolve --nameserver dns.quad9.net --old_measurement 15279140 --tcp --displayrtt  www.afnic.fr
Nameserver dns.quad9.net
[2001:67c:2218:30::24] : 473 occurrences Average RTT 142 ms
[TUCONNECT (may be a TLS negotiation error)] : 10 occurrences Average RTT 0 ms
[TIMEOUT] : 9 occurrences Average RTT 0 ms
...
Test #15279164 done at 2018-07-18T21:41:37Z
```

And finally with good old UDP :

```
%  blaeu-resolve --nameserver dns.quad9.net --old_measurement 15279140  --displayrtt  www.afnic.fr
Nameserver dns.quad9.net
[2001:67c:2218:30::24] : 471 occurrences Average RTT 237 ms
[TIMEOUT] : 24 occurrences Average RTT 0 ms
[NETWORK PROBLEM WITH RESOLVER] : 1 occurrences Average RTT 0 ms
Test #15279176 done at 2018-07-18T21:45:42Z
```

Clearly, TLS is much slower, because we have to establish a TLS session first (in real-world use, DNS-over-TLS relies on session reuse.) Note also that TCP seems faster than UDP, which will require more investigation, may be the Atlas is not taking into account the time to establish a TCP connection.

Note that another public resolver show a different picture :

```
% blaeu-resolve --requested 1000 --nameserver 1.1.1.1 --tls www.ietf.org
Nameserver 1.1.1.1
[TUCONNECT (may be a TLS negotiation error)] : 907 occurrences
[TIMEOUT] : 35 occurrences
[2400:cb00:2048:1::6814:155 2400:cb00:2048:1::6814:55] : 49 occurrences
Test #15277231 done at 2018-07-18T17:47:12Z

% blaeu-resolve --requested 1000 --nameserver 1.1.1.1 --old_measurement 15277231 www.ietf.org
Warning: --requested=1000 ignored since a list of probes was requested
Nameserver 1.1.1.1
[2400:cb00:2048:1::6814:155 2400:cb00:2048:1::6814:55] : 465 occurrences
[TIMEOUT] : 29 occurrences
[] : 1 occurrences
Test #15277240 done at 2018-07-18T17:53:30Z
```

Here, we have **more** timeouts with UDP than with TLS+TCP.