Pour se protéger de l'étranger, bloquons les accès de l'extérieur

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 août 2024. Dernière mise à jour le 31 août 2024

`https://www.bortzmeyer.org/ligne-maginot.html`

On le sait, les attaques par déni de service sont une des plaies de l'Internet, très difficiles à contrer. Quand elles sont motivés géopolitiquement, on peut souvent les lier à des pays étrangers (pas toujours à juste titre). Il est donc tentant de bloquer les attaques en bloquant l'étranger, ce que vient de faire la Cour de Cassation. Intéressant cas de géopolitique Internet.

Tout a commencé par une remarque d'une internaute vivant à l'étranger et qui s'étonnait de ne pas pouvoir accéder au site Web de la Cour de Cassation, ("*Timeout*"). Ma première réaction a été « Chez Moi, Ça Marche ». Mais je sais que l'Internet est plus compliqué que cela, je teste donc davantage, notamment avec les sondes RIPE Atlas <https://atlas.ripe.net/>, qui montrent une fois de plus leur caractère indispensable, et avec Globalping <https://www.bortzmeyer.org/globalping.html>. Et l'on voit que tout dépend du pays.

D'abord, voyons comment tester. Depuis une machine qui peut joindre le site Web de la Cour, on teste ping :

```
% ping -c 3 www.courdecassation.fr
PING www.courdecassation.fr.direct.cdn.anycast.me (80.87.226.23) 56(84) bytes of data.
--- www.courdecassation.fr.direct.cdn.anycast.me ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2055ms
```

Raté, l'hébergeur bloque ICMP echo. C'est bête mais c'est fréquent. Il va donc falloir tester uniquement en HTTPS. Sur ma machine, curl est content :

```
% curl -v https://www.courdecassation.fr/ |& more
...
* Connected to www.courdecassation.fr (80.87.226.23) port 443 (#0)
...
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384
* ALPN: server accepted http/1.1
...
> GET / HTTP/1.1
> Host: www.courdecassation.fr
> User-Agent: curl/7.88.1
...
< HTTP/1.1 200 OK
< Server: nginx
...
<!DOCTYPE html>
<html lang="fr" dir="ltr" prefix="og: https://ogp.me/ns#">
  <head>
    <meta charset="utf-8" />
<script>var _paq = _paq || [];(function(){var u ...
```

Mais depuis une machine aux États-Unis, ça échoue :

```
%  curl -v https://www.courdecassation.fr/
*   Trying 80.87.226.23:443...
* connect to 80.87.226.23 port 443 failed: Connection timed out
* Failed to connect to www.courdecassation.fr port 443 after 131838 ms: Couldn't connect to server
* Closing connection 0
curl: (28) Failed to connect to www.courdecassation.fr port 443 after 131838 ms: Couldn't connect to server
```

Sachant que les institutions françaises (et la Cour de Cassation avait été explicitement citée sur certains réseaux sociaux) ont été victimes dans les jours précédents d'attaques par déni de service politiquement motivées (apparemment en lien avec l'arrestation de Pavel Durov), on peut commencer à se douter que le résultat va dépendre du pays.

Il faudrait tester depuis davantage de points : l'Internet est vaste. Utilisons les sondes RIPE Atlas <https://atlas.ripe.net/>, via le logiciel Blaeu <https://framagit.org/bortzmeyer/blaeu>. Comme les sondes Atlas ne permettent de l'HTTP que dans des conditions très limitées, on va juste attaquer en TLS :

```
% blaeu-cert -r 100 -4 www.courdecassation.fr
73 probes reported
[/CN=www.courdecassation.fr] : 5 occurrences
[FAILED TO GET A CERT: connect: timeout] : 68 occurrences
Test #78156324 done at 2024-08-29T08:35:23Z
```

OK, certaines sondes peuvent récupérer le certificat, d'autres pas. On soupçonne déjà que ça dépend du pays donc utilisons la possibilité d'Atlas de sélectionner le pays :

```
% blaeu-cert --requested 100 -4 --country FR  www.courdecassation.fr
93 probes reported
[FAILED TO GET A CERT: connect: timeout] : 1 occurrences
[/CN=www.courdecassation.fr] : 92 occurrences
Test #78157154 done at 2024-08-29T09:18:36Z

% blaeu-cert --requested 100 -4 --country IT  www.courdecassation.fr
94 probes reported
[FAILED TO GET A CERT: timeout reading hello] : 3 occurrences
[FAILED TO GET A CERT: connect: timeout] : 91 occurrences
Test #78157186 done at 2024-08-29T09:19:28Z
```

Bref, pas de problème pour les résidents français, c'est juste l'étranger qui est bloqué. Notons toutefois que les DROM semblent exclus de la France :

```
% blaeu-cert -4 --requested 10 --country GP www.courdecassation.fr
2 probes reported
[FAILED TO GET A CERT: connect: timeout] : 2 occurrences
Test #78167255 done at 2024-08-29T11:41:39Z

% blaeu-cert -4 --requested 10 --country NC www.courdecassation.fr
5 probes reported
[FAILED TO GET A CERT: connect: timeout] : 5 occurrences
Test #78167664 done at 2024-08-29T11:50:46Z
```

Globalping <https://www.bortzmeyer.org/globalping.html> permet des requêtes HTTP. Si on lui envoie ce code JSON :

```
{
    "limit": 100,
    "locations": [{"country": "FR"}],
    "target": "www.courdecassation.fr",
    "type": "http",
    "measurementOptions": {
       "protocol": "HTTPS",
       "request": {
          "path": "/"
        }
    }
}
```

On teste en France et cela confirme le résultat des sondes Atlas ; tout marche (ou presque : la géolocalisation n'est jamais parfaite). En demandant un autre pays, tout échoue.

L'accès depuis, apparemment, le monde entier a été rétabli le 30 ou le 31 août. Tout remarche désormais.

En conclusion, il est clair que l'hébergeur de la Cour a choisi de se retrancher derrière les frontières nationales, suite aux attaques subies. Un intéressant exemple de géopolitique. Mais, par delà la question de bloquer l'accès aux gens situés à l'étranger, il n'est pas sûr que cela soit efficace du point de vue opérationnel : les attaquants professionnels n'attaquent pas depuis la machine qui est sur le bureau, ils utilisent un botnet, dont certaines machines sont en France...En outre, le blocage est fait en couche 3 (IP), contrairement aux sites de vidéo à la demande ou de commerce en ligne, qui, pour des raisons juridiques, le font en couche 7. Cela a pour conséquence l'absence de message d'erreur clair pour l'utilisateurice.

Merci à Marie-Odile Morandi pour le signalement de ce cas intéressant.

---

https://www.bortzmeyer.org/ligne-maginot.html