

From: [REDACTED]
To: [NTP Guidelines](#); [NTP Guidelines Notifications](#)
Subject: Input on the draft BEREC Guidelines on common approaches to the identification of the NTP...
Date: Wednesday, 20 November 2019 22:21:53
Attachments: [20191121-BEREC-Guidelines-Consultation.pdf](#)

Dear sirs,

I have read with great interest your draft document.

I have a few comments about it.

First, I fully agree with the Free Software Foundation Europe (FSFE) as to its comments on your draft. I have attached the document they have written, but I'm pretty sure you already got it.

Second, my own comments.

⇒ Paragraph 108 clearly pinpoints the fact that, should the NTP be located at point C, internal (private) local traffic will de facto go through the public network. The provision you add (« network operators are legally prohibited... ») are true, but we know that something being legally forbidden does not prevent anyone from doing it. And...

1/ In the tech world, one would have to use tremendous energy to prove his traffic has been spied upon by his ISP, since the NTP would very likely be a closed black box.

2/ Traffic spying may not be done by the ISP per se (as some kind of ill-conceived corporate policy) but by a rogue employee or system, an affiliate or some sub-contractor of the ISP.

3/ In the case of a major compromise of an ISP, all its customers' not-really-local traffic would be compromised. Seen another way, this would make ISPs prime targets for compromise (even more than today).

4/ In the case of a major network incident for an ISP, all its customers' local traffic could be impacted, to the point of making local traffic impossible (for example, the problem from the ISP side makes on-premises routers stop functioning).

To avoid this, the customer will add his own router just behind the ISP's one - a stupid waste of resources.

⇒ One point absent from your draft relates to failures of equipment. If the NTP is located at B or C, failure of the « ISP's hardware » (the modem or one part of modem+router, depending on the NTP's location) will mean being cut from the Internet. Since the failing equipment will be provided by the ISP, the customer cannot not have any spare. She will have to wait for a replacement equipment to reach her (here in France, this could mean a 5 to 10 days turnaround delay).

Whereas if the NTP is located at point A, all on-premise equipment will be the customer's responsibility, and she can buy spares to manage hard failures.

⇒ One point I have not seen anywhere in your draft is when the customer has several ISPs to connect her to the 'net. A lot of companies have this kind of configuration, to add some redundancy to their operations.

If the NTP is located at point A, the customer will have two modems (one


for each ISP ; there may exist multi-link modems, but I'm not aware of this) but could use only one router. This greatly simplifies the local network (configuration-, communication- and security-wise).

If the NTP is located at point C, this will mean the customer will have to buy a third router to connect the two from his ISPs. This will not only be a waste of resources, but make things more complex with routing to/from each ISP while preventing becoming an exchange point between the two ISPs.

==> In conclusion, the only place the NTP should be is at location A.

Sincerely,

--


B&A Consultants - Sécurité informatique - www.ba-consultants.fr
Tel. : +33 (0) 563 277 241 - Fax : +33 (0) 567 737 829