Gestion de réseaux quand tout est chiffré

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Gestion de réseaux quand tout est chiffré

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

afnic

Le chiffrement se répand

Le chiffrement se répand

- Pour de très bonnes raisons (surveillance par les États ou par le privé),

Le chiffrement se répand

- Pour de très bonnes raisons,
- Mais cela peut impacter des activités (pas toujours légitimes) des opérateurs réseau,

Le chiffrement se répand

- Pour de très bonnes raisons,
- Mais cela peut impacter des activités des opérateurs réseau,
- Quelles adaptations à un monde où tout est chiffré ? Fini, Wireshark.

afnic

Le chiffrement se répand

- Pour de très bonnes raisons,
- Mais cela peut impacter des activités des opérateurs réseau,
- Quelles adaptations à un monde où tout est chiffré ? Fini, Wireshark.
- Quelles conséquences pour l'opérationnel ?

afnic

Exemples de pratiques impactées par le chiffrement

Exemples de pratiques impactées par le chiffrement

- Le RFC 8404 liste des exemples (**dont certains sont abominables)**,

Exemples de pratiques impactées par le chiffrement

- Le RFC 8404 liste des exemples,
- Modification de flux HTTP (en-têtes ou contenu HTML),

afnic

Exemples de pratiques impactées par le chiffrement

- Le RFC 8404 liste des exemples,
- Modification de flux HTTP,
- Analyse de dynamiques TCP, pour optimisation,

Exemples de pratiques impactées par le chiffrement

- Le RFC 8404 liste des exemples,
- Modification de flux HTTP,
- Analyse de dynamiques TCP, pour optimisation,
- Analyse du comportement d'applications, pour déboguage et/ou optimisation,

afnic

Exemples de pratiques impactées par le chiffrement

- Le RFC 8404 liste des exemples,
- Modification de flux HTTP,
- Analyse de dynamiques TCP, pour optimisation,
- Analyse du comportement d'applications, pour déboguage et/ou optimisation,
- Analyse de trafic DNS, par exemple pour repérer certains *malwares*.

afnic

Tant mieux si le chiffrement en empêche certaines !

Tant mieux si le chiffrement en empêche certaines !

- Modifier le flux HTTP est intolérable (neutralité du réseau),

Tant mieux si le chiffrement en empêche certaines !

- Modifier le flux HTTP est intolérable,
- Regarder trop profond dans le trafic soulève bien des problèmes politiques et juridiques,

afnic

Tant mieux si le chiffrement en empêche certaines !

- Modifier le flux HTTP est intolérable,
- Regarder trop profond dans le trafic soulève bien des problèmes politiques et juridiques,
- Ça dépend beaucoup de **qui** le fait, et de sa relation avec l'utilisateur.

Le chiffrement empêche-t-il vraiment la gestion de réseaux ?

Le chiffrement empêche-t-il vraiment la gestion de réseaux ?

- C'est ce que laisse entendre le RFC 8404,

Le chiffrement empêche-t-il vraiment la gestion de réseaux ?

- C'est ce que laisse entendre le RFC 8404,
- Déjà, ça dépend des couches :

Le chiffrement empêche-t-il vraiment la gestion de réseaux ?

- C'est ce que laisse entendre le RFC 8404,
- Déjà, ça dépend des couches :
  - Couche 1 : on voit toujours les signaux,

Le chiffrement empêche-t-il vraiment la gestion de réseaux ?

- C'est ce que laisse entendre le RFC 8404,
- Déjà, ça dépend des couches :
  - Couche 1 : on voit toujours les signaux,
  - Couche 2 : on voit toujours les trames et leur taille,

afnic

Le chiffrement empêche-t-il vraiment la gestion de réseaux ?

- C'est ce que laisse entendre le RFC 8404,
- Déjà, ça dépend des couches :
  - Couche 1 : on voit toujours les signaux,
  - Couche 2 : on voit toujours les trames et leur taille,
  - Couche 3 : on voit toujours les adresses IP et le protocole de transport, et normalement **l'opérateur s'arrête là**,

afnic

Le chiffrement empêche-t-il vraiment la gestion de réseaux ?

- C'est ce que laisse entendre le RFC 8404,
- Déjà, ça dépend des couches :
  - Couche 1 : on voit toujours les signaux,
  - Couche 2 : on voit toujours les trames et leur taille,
  - Couche 3 : on voit toujours les adresses IP et le protocole de transport, et normalement **l'opérateur s'arrête là**,
  - Couche 4 : avec SSH et TLS, on voit toujours les bits SYN, RST, FIN... On voit toujours les ports. IPsec et QUIC les masquent.

afnic

Ne pas tout mélanger

Ne pas tout mélanger

- Le RFC 8404 parle d'opérateurs réseaux qui déboguerait des problèmes de vidéo,

Ne pas tout mélanger

- Le RFC 8404 parle d'opérateurs réseaux qui déboguerait des problèmes de vidéo,
- Il confond les fournisseurs de services applicatifs et les « vrais » opérateurs,

Ne pas tout mélanger

- Le RFC 8404 parle d'opérateurs réseaux qui déboguerait des problèmes de vidéo,
- Il confond les fournisseurs de services applicatifs et les « vrais » opérateurs,
- Si on gère un service (vidéo-conférence, par exemple), on contrôle les extrêmités et on peut leur demander d'afficher les informations,

afnic

Ne pas tout mélanger

- Le RFC 8404 parle d'opérateurs réseaux qui déboqueraient des problèmes de vidéo,
- Il confond les fournisseurs de services applicatifs et les « vrais » opérateurs,
- Si on gère un service, on contrôle les extrêmités et on peut leur demander d'afficher les informations,
- Un problème reste ouvert : beaucoup d'applications ne font pas cela bien. Il y a du travail à faire ici.

afnic

Ne pas tout mélanger

- Le RFC 8404 parle d'opérateurs réseaux qui déboguerait des problèmes de vidéo,
- Il confond les fournisseurs de services applicatifs et les « vrais » opérateurs,
- Si on gère un service, on contrôle les extrêmités et on peut leur demander d'afficher les informations,
- Un problème reste ouvert : beaucoup d'applications ne font pas cela bien.
- Résumé : mauvaise campagne visant à limiter le chiffrement.

afnic

Merci !

www.afnic.fr
contact@afnic.fr