

1^{ère} réunion avec Julien MONTAVONT
L2S4 PRDS
14/02/2024

Présent-es :

- Julien MONTAVONT
- Carine WAKIM
- Maxime ZINGRAFF

Cadre : Salle de réunion équipe réseaux, de 11h15 à 12h15

Ordre du jour prévisionnel : il n'avait pas été établi d'ordre du jour clair

1. Présentation générale de l'avancement

Nous présentons l'état actuel de nos recherches en bloc, ainsi que notre plan prévisionnel :

- I. Les NAT et leur fonctionnement :
 - DMZ
 - A. L'objectif principal des NAT
 - 1. Modèle OSI (rapidement)
 - 2. Qu'est-ce qu'un NAT ?
 - 3. La ou les raison(s) derrière la naissance des NAT
 - B. Les 3 types de NAT
 - 1. Les NAT statiques
 - 2. Les NAT dynamiques
 - 3. Les PAT (NAPT)
 - a) Statique uni et bidirectionnel
 - b) Dynamique bi-directionnel (le plus utilisé) dont NAT Overload (ou masquerading)
 - 4. CGNAT / NAT444
 - 5. NAT64 (IPv6) : traduction de IPv6 à IPv4 (forcément dynamique) ou IPv4 à v6 (NAT46)
 - 6. Fonctionnement technique de la traduction (traduction de l'en-tête des paquets TCP/UDP)
- II. Les NAT : des outils de sécurité ?
 - A. Les NAT statiques et les NAT dynamiques ne sont pas concernés
 - B. Les PAT, un outil pour sécuriser les réseaux
- III. Contournement des NATs
 - A. Les problèmes techniques posés par les NAT (les raisons de contournement des PAT)
 - 1. Besoins de temps de réponse (VoIP, ...) et de sécurité (protocoles bout à bout)
 - 2. Pas de traduction de l'en-tête pour certains protocoles (à check)

B. Les techniques de contournement

1. UPnP/PCP, ICE (STUN/TURN), VPN, DMZ (pour rétablir connectivité)

Julien MONTAVONT nous conseille de creuser davantage la partie sur les NAT Dynamiques, et notamment le fonctionnement technique et l'ordre dans lequel se déroule l'établissement d'une connexion.

Nous évoquons les CGNAT (ou NAT 444). M. MONTAVONT nous conseille de ne pas évoquer ce sujet, étant donné que les FAI communiquent peu sur le sujet et que ce n'est pas un aspect clé du sujet.

Selon M. MONTAVONT, le point du retour du paquet quand on utilise un NAT et surtout un port dynamique est un aspect clé. C'est notamment le cas pour les visioconférences, les appels VoIP ou encore le protocole FTP qui utilisent des ports dynamiques. L'aspect sécuritaire est un autre point très important.

Il nous suggère donc de réorganiser notre plan de la manière suivante :

- I. Fonctionnement des NAT
- II. Problèmes de connectivités
- III. Aspects sécuritaires des NAT

Nous posons une question sur le fonctionnement technique des NAT. La partie du remplacement des adresses dans l'en-tête TCP/UDP n'est pas la partie la plus lourde de la traduction, c'est surtout la mise à jour du contrôle d'erreur qui ralentit le processus. Mais étant donné la rapidité des connexions à l'heure actuelle, la mise en place des NAT n'est pas un facteur déterminant pour la rapidité d'une connexion.

Carine WAKIM demande des détails sur les apports sécuritaires des NATs. M. MONTAVONT nous explique que les PAT permettent de changer les ports "de base" et donc de sécuriser certains protocoles, alors que les NAT sans traduction de ports permettent d'avoir des appareils sur le réseau local coupés d'Internet. Ces deux aspects sont le cœur de la sécurité apportée par les NAT. Les NAT (indépendamment de leur type) permettent donc de fournir une fine couche de sécurité en masquant les adresses IP privées. Les PAT, quant à eux, ajoutent une couche de sécurité supplémentaire liée à la traduction des ports (en filtrant les paquets entrants).

Maxime ZINGRAFF pose une question sur les sources que l'on peut utiliser. La source "suprême" est le RFC : c'est une norme adoptée par tous, et qui est donc irréfutable. Une source de bonne qualité peut aussi être des articles publiés dans les revues IEEE. Les normes IEEE, quant à elles, concernent plus la couche physique que la couche transport, elles ne nous seront donc pas utiles.

M. MONTAVONT appuie sur le fait de distinguer le sous ensemble des sources utilisées parmi l'ensemble des sources lues. Il faut garder trace de tout ce que l'on lit, mais pas forcément le citer.

Dans notre rapport ou dans nos présentations, nous risquons de nous retrouver avec beaucoup de RFC. Il n'est pas grave d'avoir une majorité de RFC dans ses sources, étant donné que c'est la "source parfaite" mais il faut alors expliquer cette surreprésentation.

M. Z. demande le niveau de détail nécessaire pour la description des protocoles. M. MONTAVONT indique qu'il n'est pas forcément nécessaire d'aller jusqu'à l'étude de l'en-tête du protocole mais qu'une explication détaillée est nécessaire. Il est inutile de citer seulement un protocole sans rentrer dans le détail ; autant ne pas le citer du tout.

Il peut être intéressant de détailler les interactions entre les acteurs et également de construire des chronogrammes.

M. MONTAVONT évoque les types de NAT : A, B, et C. Il nous suggère d'approfondir ce sujet et, par exemple, de faire un sondage sur nos camarades pour connaître le type de NAT utilisé à la maison, en fonction des différences entre FAI. Nous indiquons que nous avons trouvé plusieurs sources contradictoires et que nous allons donc approfondir le sujet.

Pour conclure, M. MONTAVONT nous demande de créer un dépôt Git où nous devrions déposer

- Les comptes-rendus des réunions
- L'agenda prévisionnel et minuté des prochains rendez-vous
- Les sources lues et pertinentes
- Les diaporamas des présentations d'avancements bi-hebdomadaires

Nous convenons également d'un prochain rendez-vous le 21/02/2024 à 11h.