

Plan du sujet : version du 30/04/2024

- I. Remerciements
- II. Introduction
 - A. Problème : la pénurie d'adresses IPv4
 - B. Les NAT : une solution provisoire
 - C. Pourquoi se poser cette question : le filtrage fourni (par effet de bords) par les NAT → Les NAT deviennent à la fois une barrière protectrice mais aussi une entrave à la communication → Mais ces barrières sont-elles infranchissables ?
- III. Network Address Translators : philosophie & nomenclature */!\ ne rien oublier*
 - A. Le rôle et ce que sont les NAT
 - 1. Pourquoi les NAT (manque IPv4)
 - 2. Philosophie générale
(*Position dans la couche OSI*)
 - 3. Comment est-ce qu'ils pallient le manque d'adresses IPv4 ?
 - B. Types informels (A, B, C)
 - C. RFC 4787
 - 1. Différents types & avantages sécuritaires sécuritaires
- IV. Problèmes engendrés
 - A. Connexion entrante inconnue dans un mappage non-EIM
 - B. Situations problématiques :
 - 1. Un service est hébergé derrière un NAT ← Problème (exemple possible)
- V. Méthodes de contournement
 - A. Relaying
 - 1. TURN
 - B. Hole punching
 - 1. STUN
 - C. Conclusion : ICE : réunion des deux (en 2 mots)
UPnP ??? → voir avec M. MONTAVONT
- VI. Le Futur des NAT
 - A. Statu quo
 - B. Seulement IPv6 : plus de NAT car plus nécessaire (pas d'apports sécuritaires)
 - C. Entre-deux : méthodes d'interconnexions
- VII. Conclusion

Originellement conçus pour pallier le manque d'adresses IP → considérés comme outils sécuritaires alors que ce n'est pas vraiment le cas → cohabitation avec IPv6 et disparition à terme