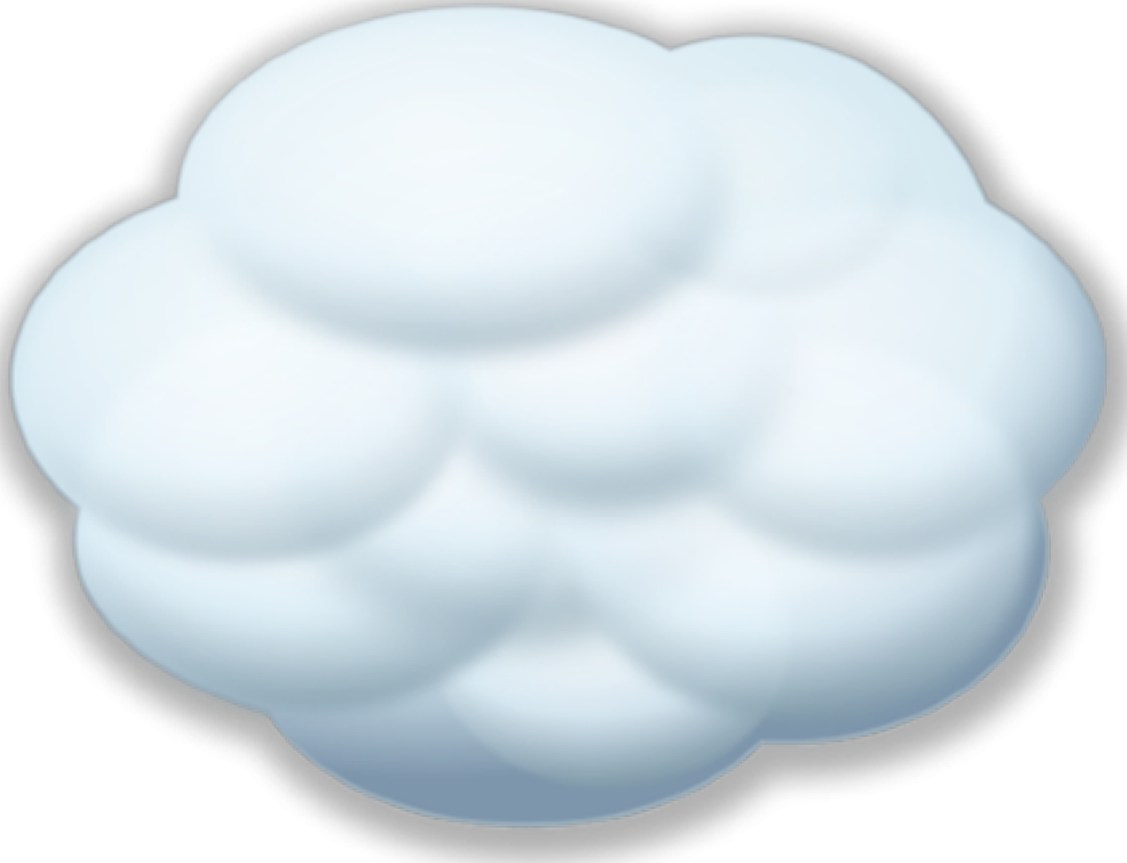
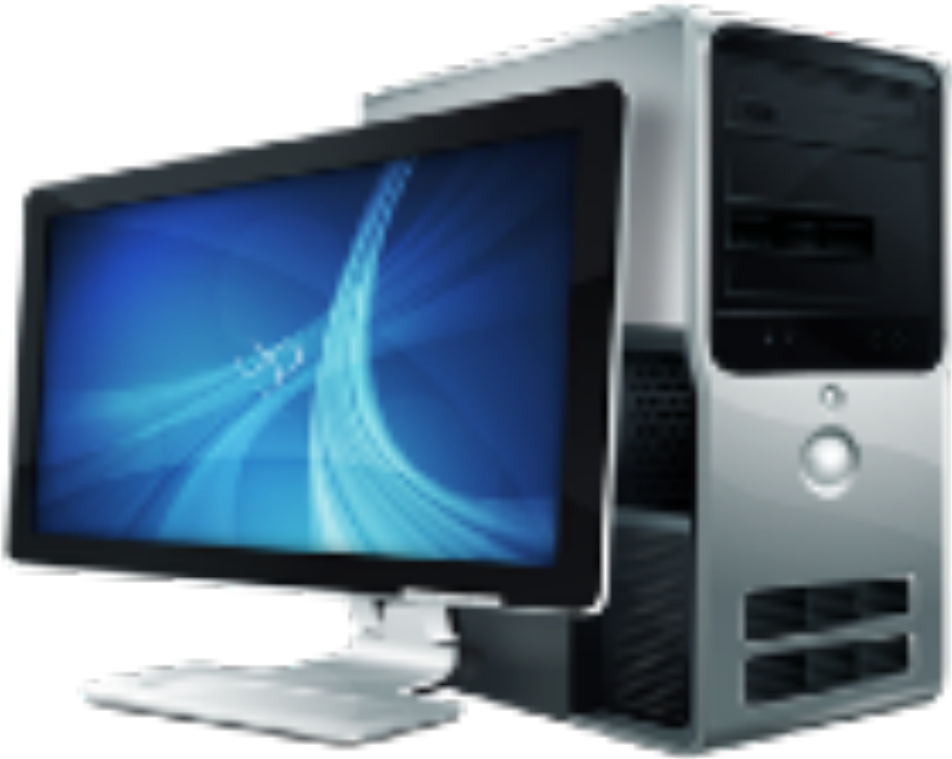




: Principe de fonctionnement

DNS

www.entreprise.fr

Connexion sur www.entreprise.net:80 ?

Adresse IP de www.entreprise.net ?

Connexion…

Connexion établie !

Fin de connexion

Serveur Socks

Socks

Exploitation

Contournement de pare-feu

Socks : Principe de fonctionnement

1 : Le client se connecte et s'authentifie au serveur Socks

2 : Le client demande à se connecter sur www.entreprise.fr en 80/TCP

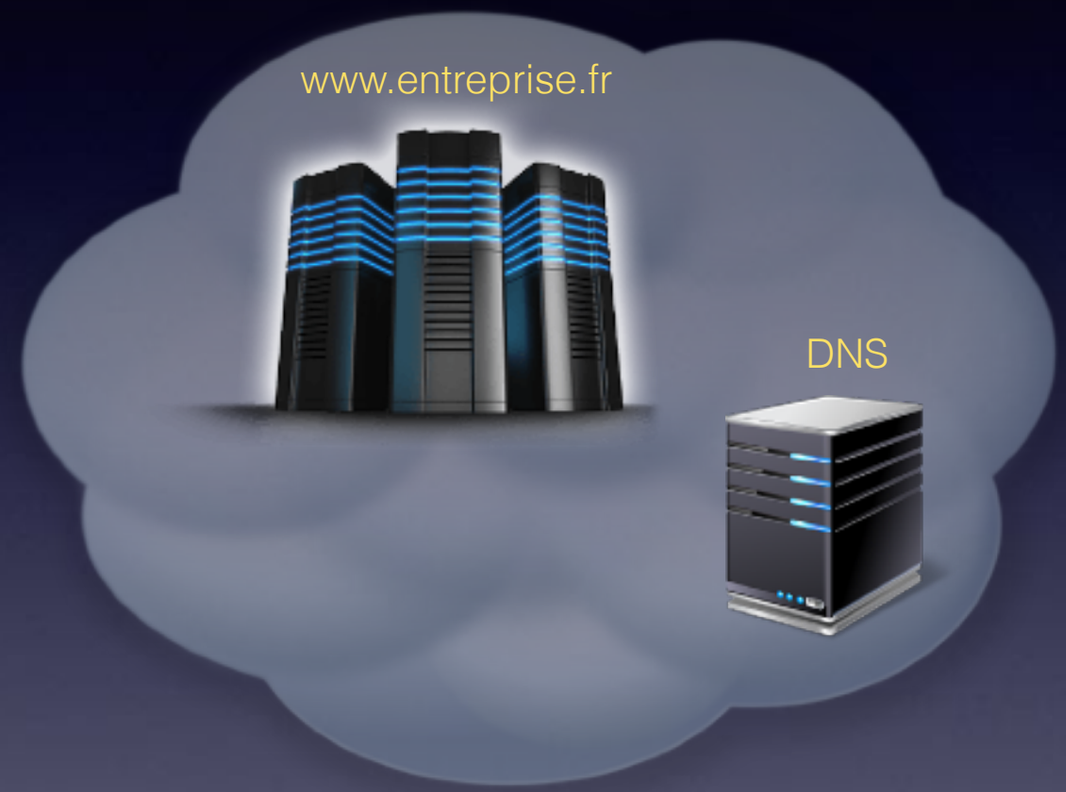
3 : Le serveur demande à son serveur propre DNS l'adresse IP de www.entreprise.fr

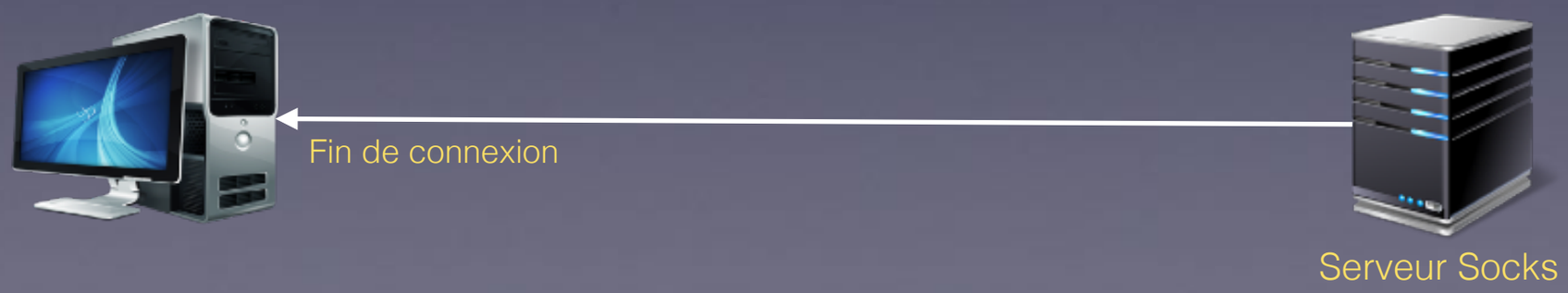
4 : Le serveur tente de se connecter sur 80/TCP de @IP

<u>2 possibilités :</u>

✔ 5 : La connexion est établie !
- Le serveur informe le client que la connexion est établie ;
- Le client envoie ses données au serveur en leur ajoutant une entête Socks.

✖ 5 : La connexion n'est pas établie. Le serveur ferme la connexion TCP avec le client.





Exploitation

Contournement de pare-feu

Rebonds : Socks

Avantages :

- La résolution de nom est réalisée par le serveur DNS du serveur Socks ;
- Possibilité de se connecter à n'importe quelle machine joignable à partir du serveur Socks;
- Les communications à destination de www.entreprise.net provient du serveur et non de la machine cliente ;
- La confidentialité des communications via un serveur Socks dépend de son tunnel. (SSH).

Inconvénients :

- L'UDP n'est pas prise en compte par OpenSSH.