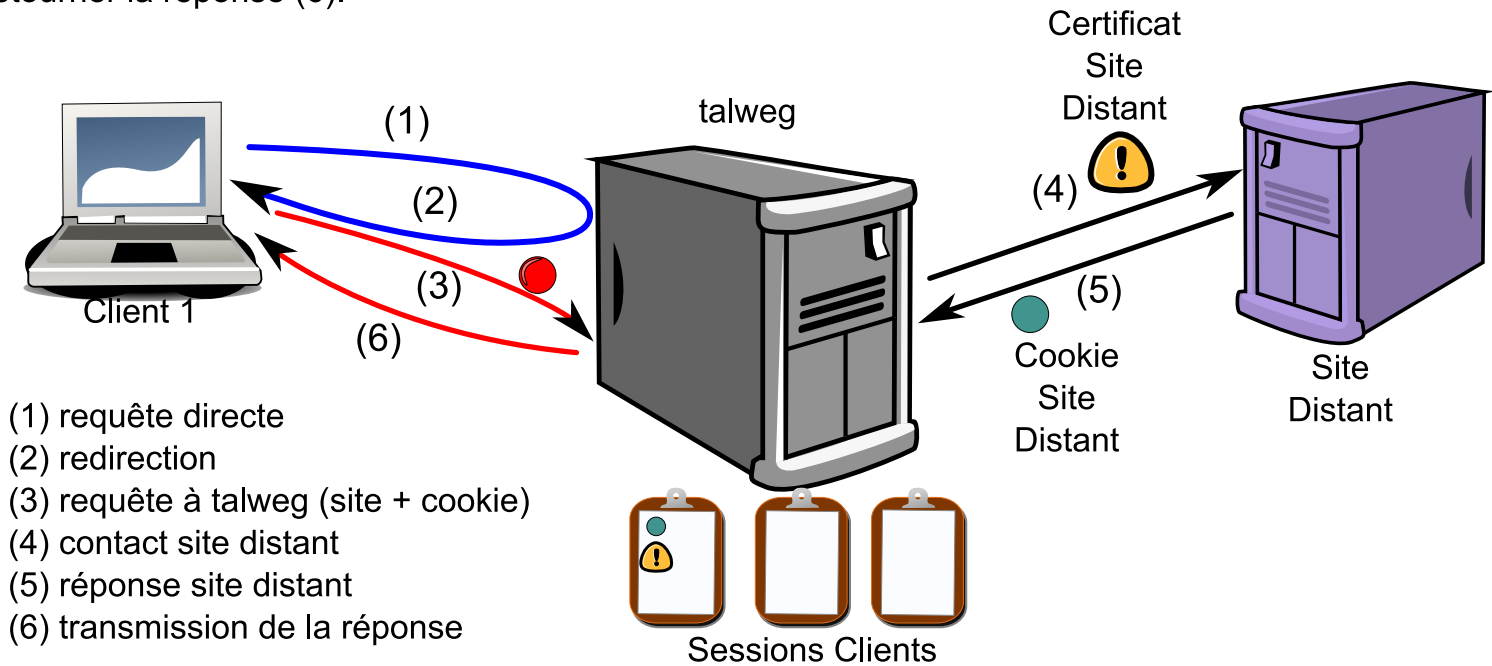


Le principe de base de cette solution est, en évitant l'identification par adresse IP/MAC jugée peu sécurisée, d'utiliser une authentification par cookie chiffré. Procédé utilisé pour les paiements bancaires. Afin de garantir qu'une requête provienne d'un utilisateur identifié, celle-ci doit contenir le cookie d'authentification.

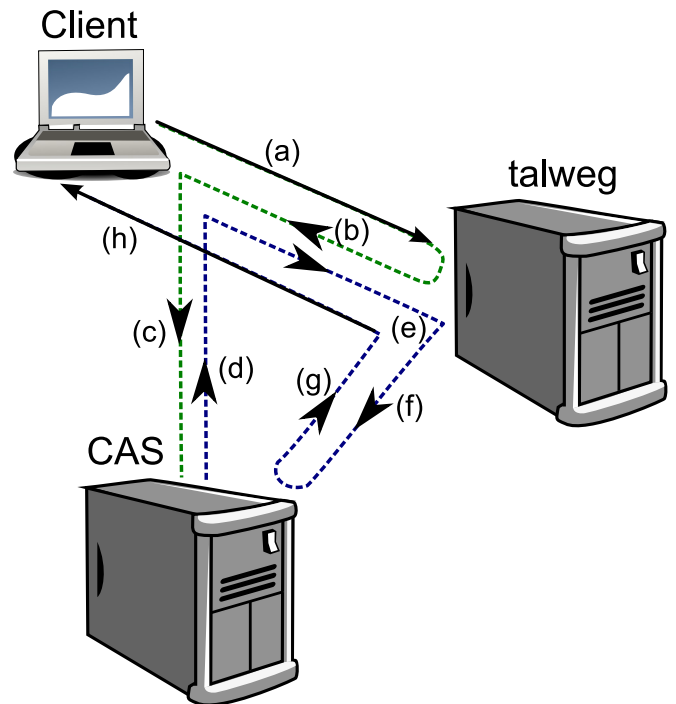
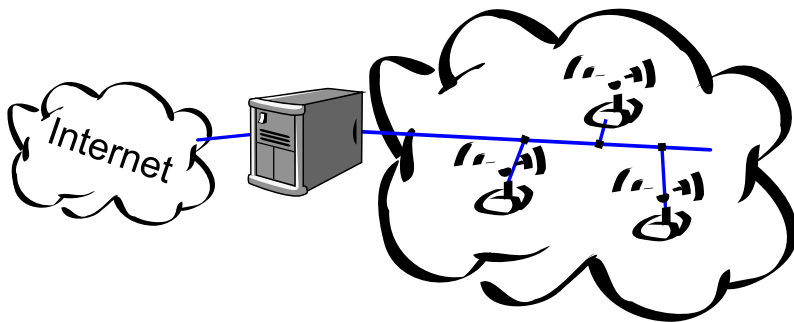
La technique consiste donc à utiliser les « redirections HTTP » (1) (2) pour contraindre les requêtes à utiliser un canal virtuel sécurisé (3) SSL à destination du proxy/gateway (talweg). Celui-ci a pour charge de vérifier la validité du cookie, d'exécuter la requête (4) (5) pour le client et de lui retourner la réponse (6).



AUTHENTIFICATION CAS

A l'Université de Metz, nous utilisons le SSO CAS. Il est basé sur le principe d'échange et de validation de tickets (figure de droite).

Cependant, toutes les méthodes d'authentification sont envisageables (RADIUS, LDAP, Fichier, ...)



Le réseau sans fil est restreint dans un VLAN. talweg est la seule sortie possible.

Les équipements (manageables) sont configurés de telle sorte que les connexions entre machines du réseau sans fil sont impossibles (intra et extra bornes).