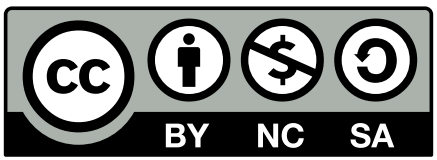
université de BORDEAUX

Etude et Implémentation du Single Packet Authorization

Cédric Céola - Jacques Monin
<cedric.ceola@etu.u-bordeaux.fr>

Master CSI, Université de Bordeaux, France

17 mars 2015



Plan

Plan

- Se base sur une contexte réseaux fonctionnels apportant certains services à ses clients.
- Ajout d'un environnement de sécurité.

- Se base sur une contexte réseaux fonctionnels apportant certains services.
- Ajout d'un environnement de sécurité.

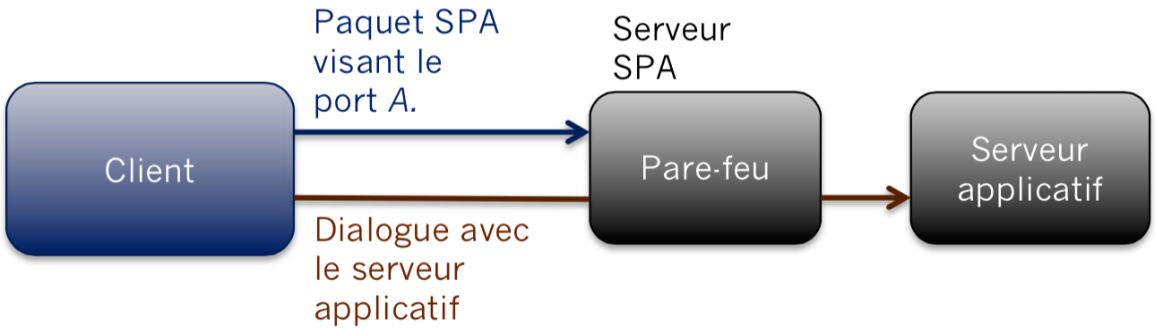
SPA : ***S****ingle* ***P****acket* ***A****uthorization:*

- Demande d'un client à un serveur SPA, intermédiaire d'un applicatif.

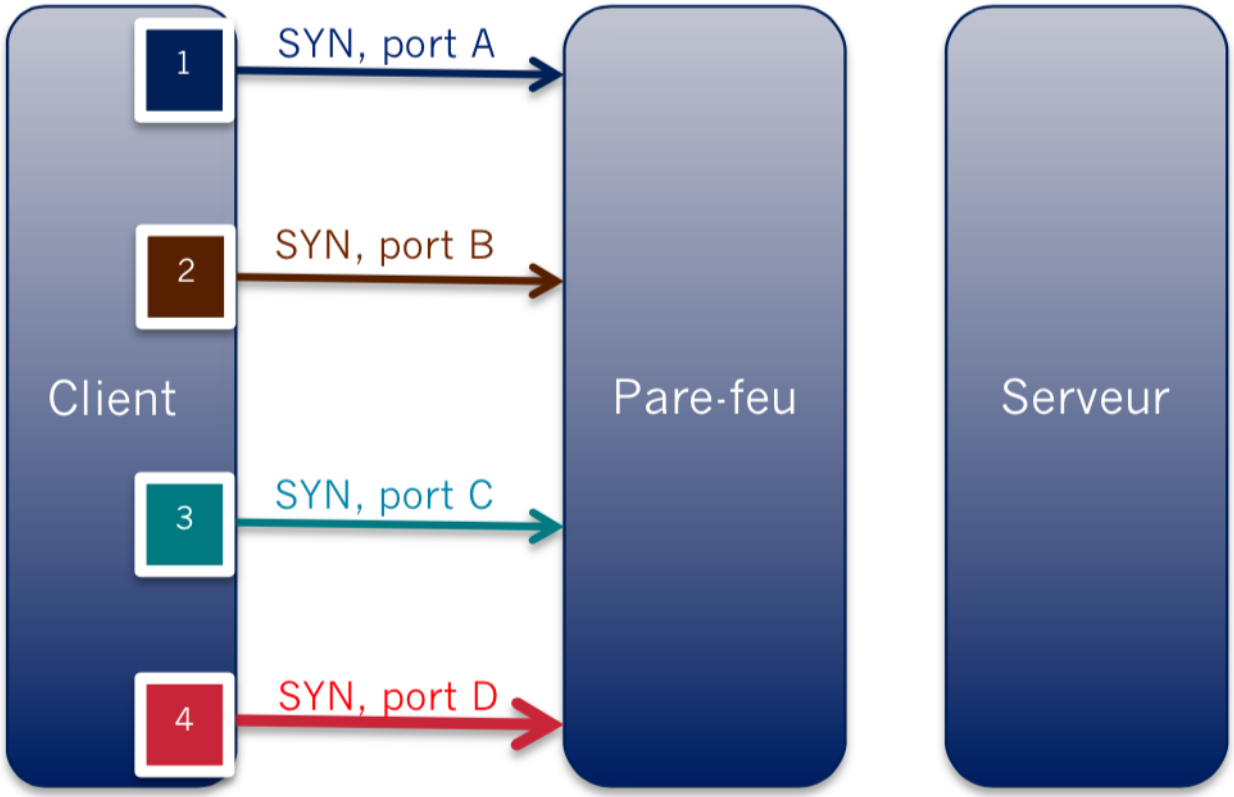
- Se base sur une contexte réseaux fonctionnels apportant certains services.
- Ajout d'un environnement de sécurité.

SPA : ***S****ingle* ***P****acket* ***A****uthorization:*

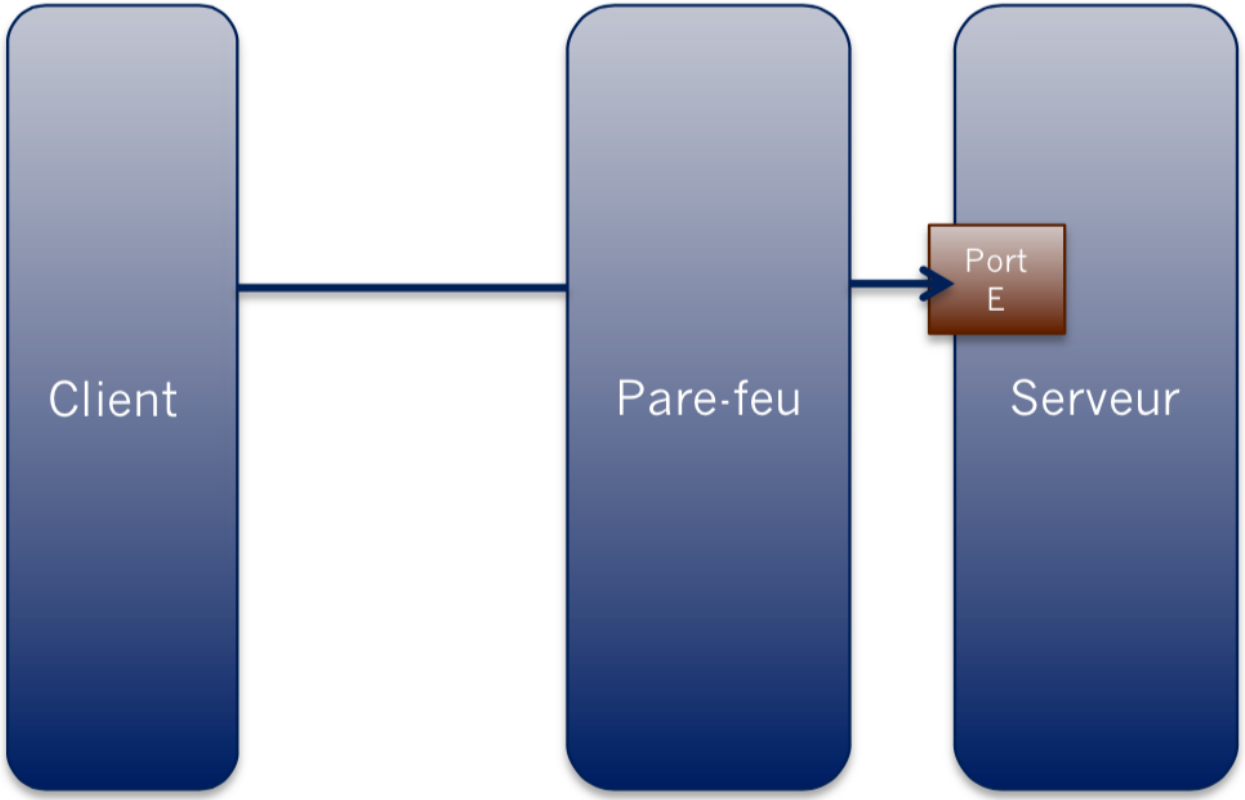
- Demande d'un client à un serveur SPA, intermédiaire d'un applicatif.
- Le serveur SPA reçoit cette demande est décide de l'attribution du laisser-passer.



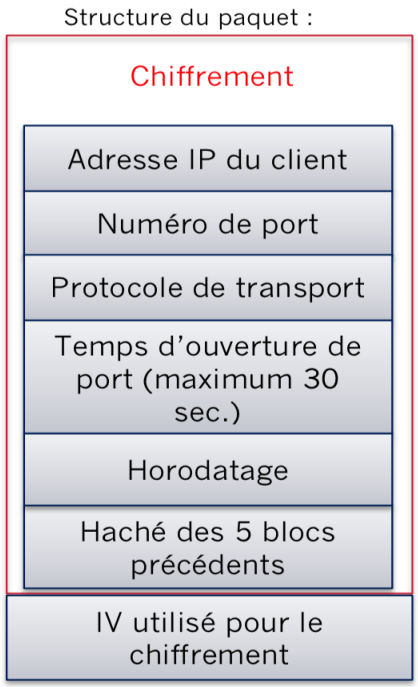
- Principe identique au *Port Knocking*.



- Principe identique au *Port Knocking*.



Plan



Adresse IP du client : Cette adresse nous sert à nous assurer que le client émetteur du paquet et aussi celui qui l'a chiffré (authenticité).

Numéro de port : Ce champ correspond au port logiciel du serveur applicatif auquel le client souhaite obtenir l'accès.

Protocole de transport : Si la demande d'accès est validée, le client pourra communiquer avec le serveur via le protocole de transport spécifié dans ce champ.

Temps d'ouverture du port : Par défaut, le serveur SPA autorise de laisser passer les paquets demandés pour une période maximale de 30 secondes. Le client peut cependant demander l'accès pour un période plus restreinte.

Horodatage : Ce champ sert à différencier les demandes successives d'un même client. En effet, sans ce champ, un client produisant deux demandes similaires de laisser passer à 10 minutes d'intervalles, génèrerait deux paquets identiques, rendant ainsi le rejeu facile à exploiter.

Haché des 5 blocs précédents : Ce haché sert, au niveau du serveur SPA, à vérifier l'intégrité de ces blocs. Il est aussi utile à la détection du rejeu.

Chiffrement : les 6 blocs précédents sont ensuite chiffré par un système de chiffrement symétrique à clé partagée par le serveur et un de ses clients afin de préserver l'authenticité.

IV utilisé pour le chiffrement : Notre système de chiffrement utilisant un IV, le client l'envoi au serveur en clair.

Plan

PROTECTION

Plan

Livres et références I

Questions ?