DNS – Serveurs multiples et sécurité

420-2S5-EM

Serveur 1 : Services intranet

Retour sur différents concepts:

- Un serveur DNS a pour objectif de traduire des noms de domaine en adresse IP et des adresses IP en noms de domaine.
- Il réalise ce petit exploit grâce aux enregistrements qu'il possède ou en transférant la requête vers des serveurs DNS qui mèneront d'une manière ou d'une autre vers une résolution.
- Les enregistrements du serveur DNS sont stockés dans des zones de recherches directs ou inverses.

Le DNS est un service critique! 

- Le service de résolution de nom DNS est crucial. Sans ce service, l'accès internet d'une entreprise ou même ses différents services d'administration pourraient ne plus fonctionner convenablement.

- On aura donc tendance à mettre plus d'un serveur DNS dans le réseau local afin de profiter d'une redondance du service.

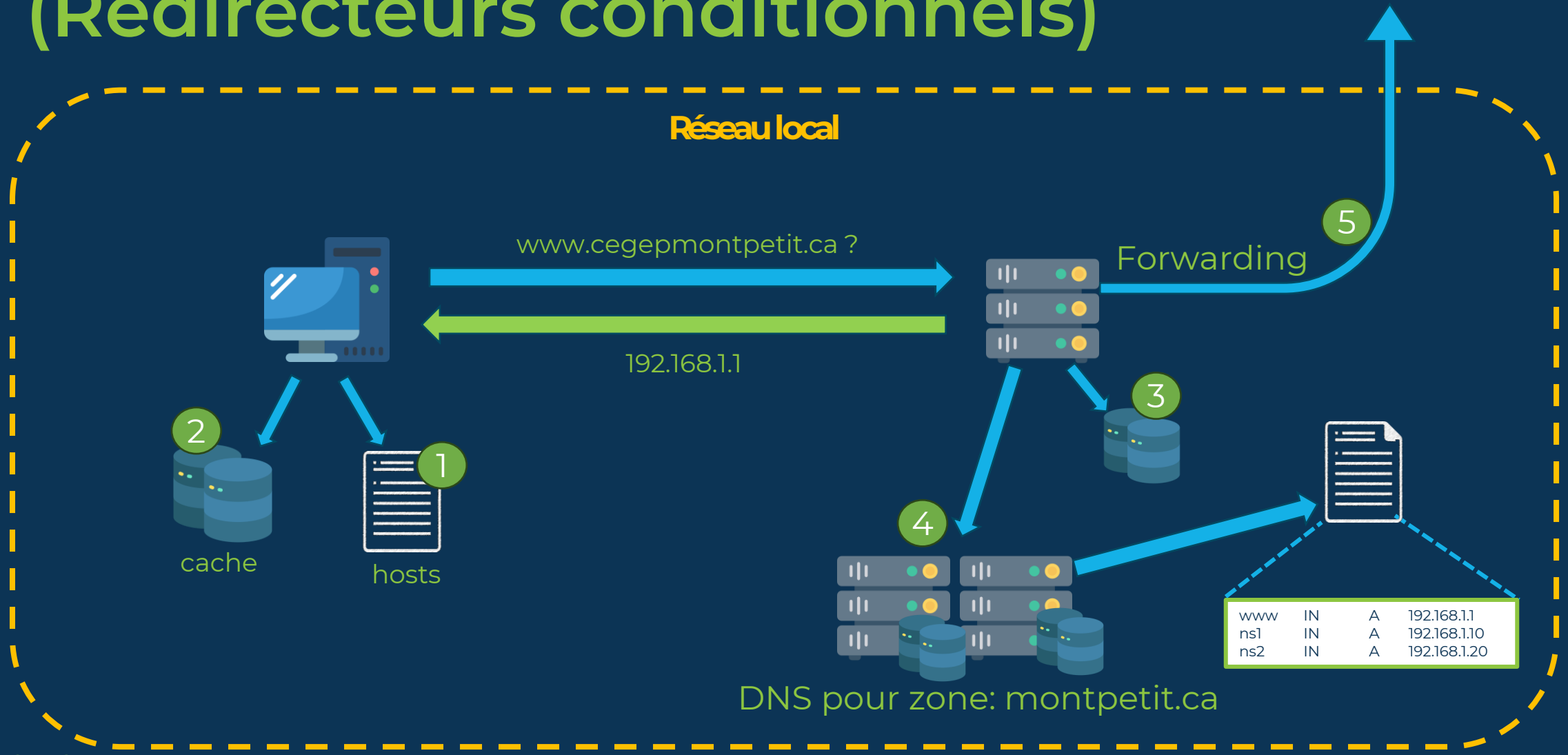
- La redondance sera donc un gage de haute disponibilité.

Gestion de la charge de travail

- Récemment, nous avons parlé des redirecteurs. Sachez qu'il est possible d'appliquer des conditions à nos redirecteurs. En présence de plusieurs serveurs DNS, cela nous permet de gérer le travail de chacun de ceux-ci.

- Par exemple: Nous pourrions avoir deux serveurs DNS pour les requêtes sur le nom de domaine local et un serveur de cache DNS pour les requêtes externes.

Exemple de gestion de charge (Redirecteurs conditionnels)



ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

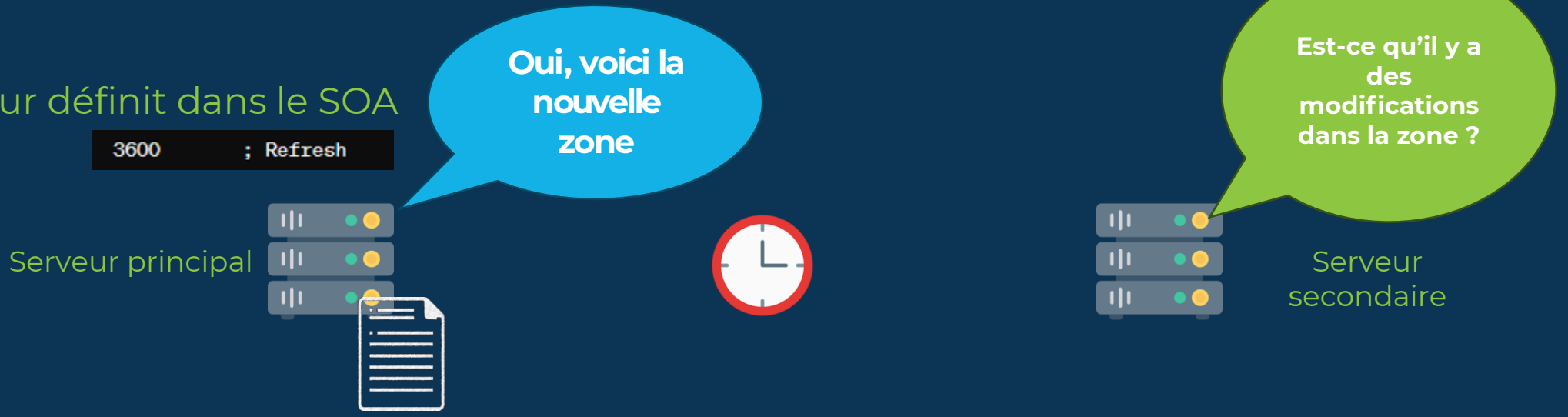
Hiérarchie principal-secondaire(s)

- Dans l'exemple précédent, deux serveurs DNS géraient la zone cegepmontpetit.ca
- Comme nous l'avons vu précédemment, même s'ils se partagent la zone, un seul serveur DNS peut effectuer des modifications sur les enregistrements, le serveur principal.
- Il y aura donc des transferts de zone qui s'effectueront entre le serveur principal et le, ou les, serveurs secondaires.

Fonctionnement du transfert:
Basé sur le temps

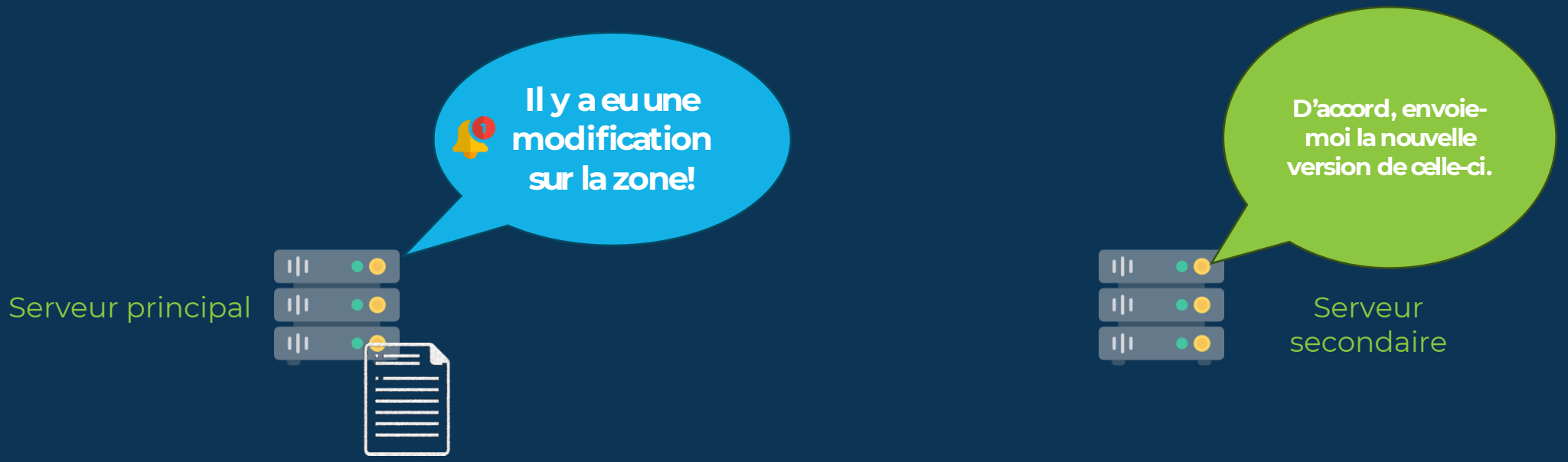
Valeur définit dans le SOA

```
3600          ; Refresh
```



ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

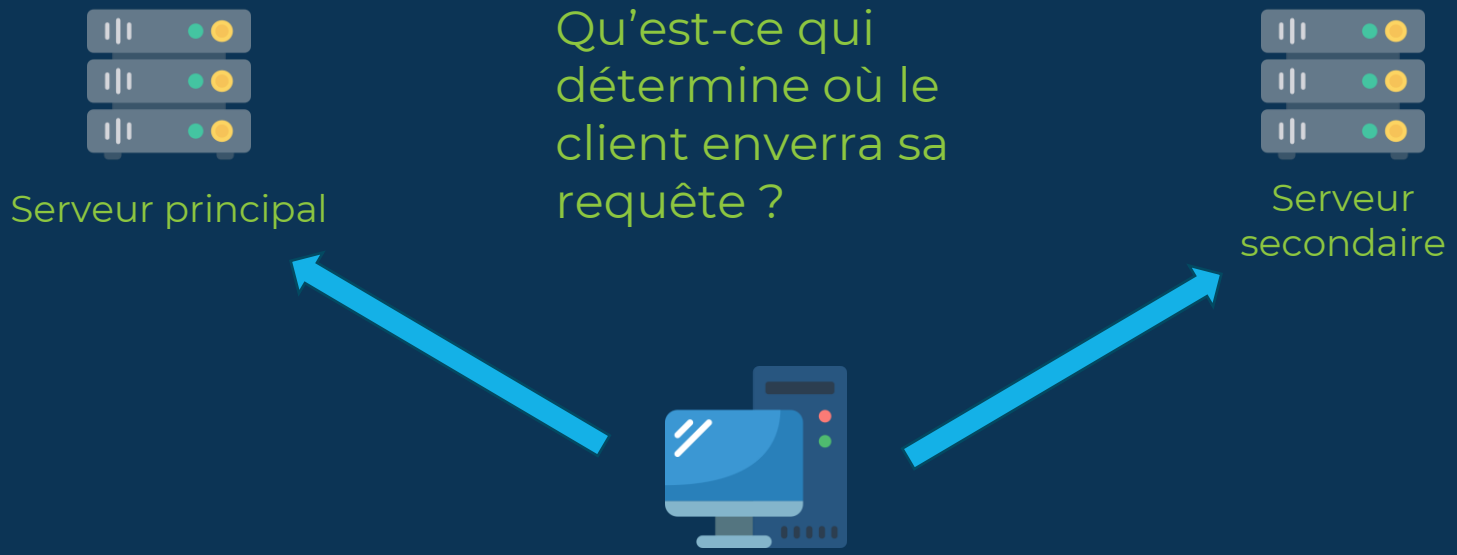
Fonctionnement du transfert:
Basé sur les notifications



ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

Sélection du serveur DNS

Sur quoi un client se base pour sélectionner l'un ou l'autre des serveurs DNS configurés ?



Sélection du serveur DNS côté client

Windows:

L'algorithme de sélection du serveur DNS est à code fermé sur Windows. Cela dit, on peut présumer que Windows sélectionnera le serveur DNS en fonction du temps de réponse d'une requête ainsi qu'en fonction de la disponibilité du serveur DNS.

Linux:

Sur Linux, l'algorithme de sélection du serveur DNS peut être géré minimalement. En effet, on peut indiquer à Linux d'effectuer une rotation entre chaque requête DNS. Cela aura pour effet de distribuer la charge de travail de résolution entre les différents serveurs.

Sécurité des serveurs DNS

- S’attaquer à un serveur DNS peut s’avérer très payant pour un pirate informatique. En effet, une seule attaque réussit sur un serveur DNS peut mener à la corruption de plusieurs ordinateurs.

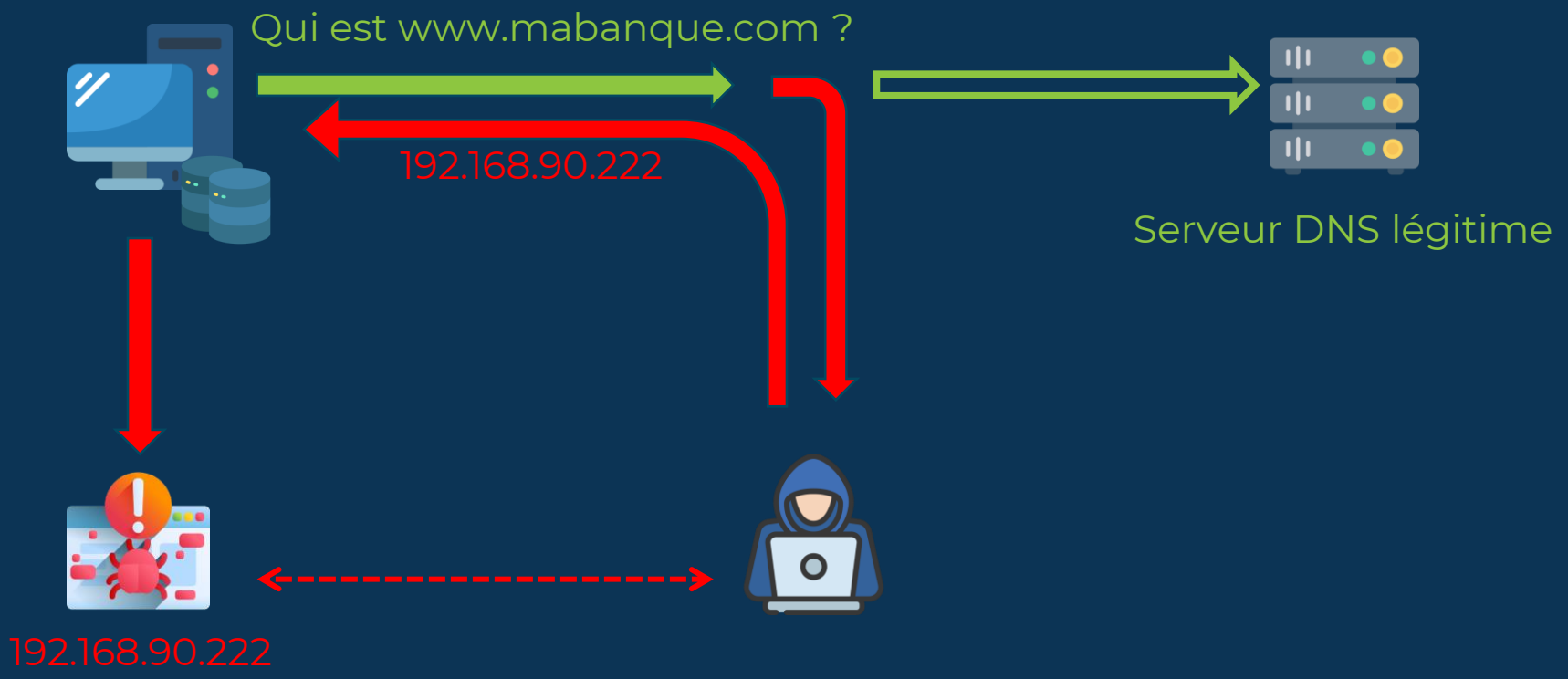
- Pour bien contrer les risques liés à la sécurité des DNS, il faut d’abord en saisir les concepts en détails.

DNS Hijacking

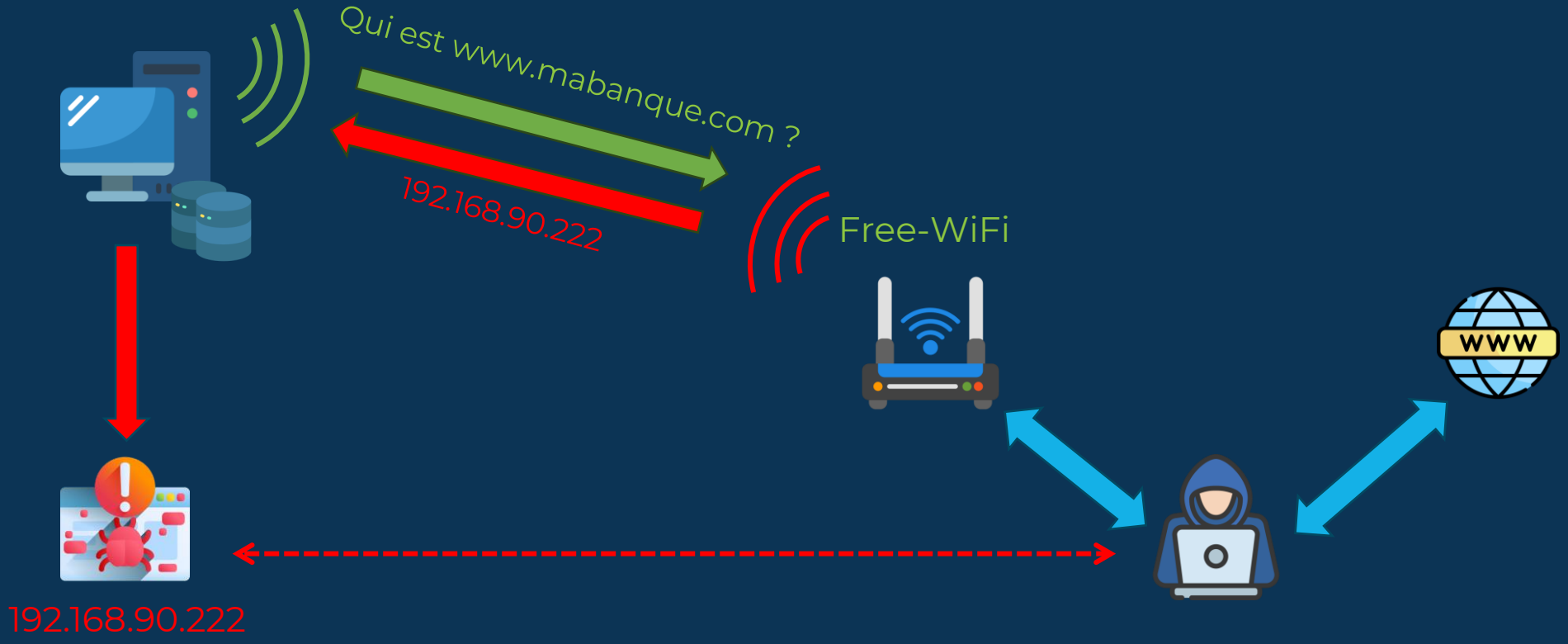
Le DNS « hijacking » est un type d'attaque qui vise les clients, et non les serveurs DNS. À l'aide de différentes méthodes, les attaquants essaieront de mettre en place un faux serveur DNS qui répondra aux requêtes légitimes des clients afin de les rediriger vers des sites frauduleux.

Si les clients stockent la réponse du faux serveur DNS dans leur mémoire cache, cette attaque pourrait alors s'étirer dans le temps.

Exemple de DNS « hijacking » #1



Exemple de DNS « hijacking » #2



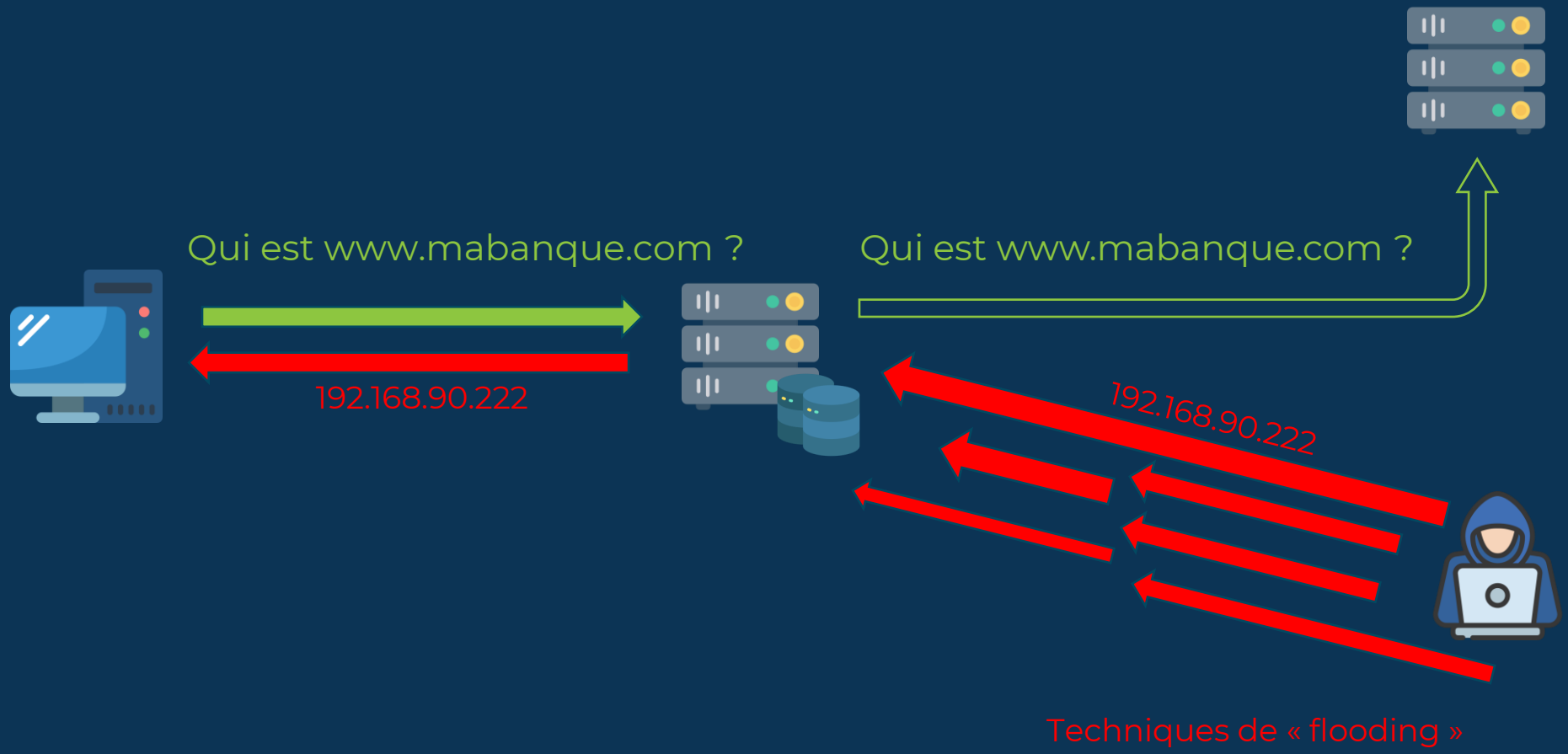
ÉDOUARD MONTPETIT
CÉGEP D'AVENIR

DNS Poisonning

Le DNS « poisonning» est un type d'attaque qui vise les serveurs DNS de type cache. À l'aide de différentes méthodes, les attaquants essaieront d'empoisonner la mémoire cache d'un serveur DNS pour que celui-ci puisse, à son tour, répondre faussement aux requêtes DNS.

Lorsque ce type d'attaque réussit, elle fait plusieurs victimes d'un seul coup.

Exemple de DNS « poisonning »



Sécuriser les serveurs DNS

- La technologie DNSSEC (DNS Security Extension) a été instaurée pour éviter que ce genre de risques en lien avec la sécurité des DNS soit exploité.

- Avec DNSSEC, il est possible de « signer » numériquement les enregistrements DNS d'une zone. Cette façon de procédé empêchera toute mise-à-jour ou modification des enregistrements de la zone sans d'abord y avoir été expressément autorisé.

Sécuriser les serveurs DNS

Les transferts de zones entre serveurs DNS principaux et secondaires peuvent également être sécurisés grâce à une autre technologie de signature que l'on nomme « transaction signature ». Cette dernière technologie n'est pas intégrée à ce qu'on appelle DNSSEC, cependant les deux technologies peuvent être complémentaire.