“Serveur Uniquement Autoritaire” & TSIG

Atelier ccTLD

Dakar, 7-10 décembre 2005

Document de Alain Patrick AINA
Traduit par Alain Patrick AINA

Différents types de serveurs

Plusieurs types de serveurs de noms

- Serveurs autoritaires
  - Maître (primaire)
  - Esclave (secondaire)
- Les serveurs cache
  - Aussi “cache forward”
- Mixage de fonctionnalités

Pourquoi séparer les fonctionnalités(1)?

Les données autoritaires et non autoritaires sont destinées à différents groupes de clients

- Afin de servir des données autoritaires à l'Internet, les NS doivent être en dehors du pare-feu
- Les caches doivent généralement être placés derrière un pare-feu pour les protéger comme les abus externes.

Servir les données autoritaires est plus important que servir les données du cache; surtout pour vous les opérateurs de noms de domaine nationaux.

Pourquoi séparer les fonctionnalités(2)?

Les serveurs cache peuvent être empoisonnés

- Si un pirate arrive à faire accepter des ER falsifiés avec un grand TTL à votre serveur cache, des données invalides peuvent être utilisées pour servir des données autoritaires.

Certaines attaques de déni de service et de “buffer overrun” réussissent mieux sur les serveurs cache.

Pourquoi séparer les fonctionnalités(3)?

Les serveurs autoritaires peuvent servir les données autoritaires(constantes en taille) plus efficacement si les données du cache ne monopolisent pas les ressources systèmes.

- Les clients récursifs utilisent de la mémoire (jusqu'à 20kb/s)
- Les serveurs cache utilisent de la mémoire pour garder les données
- Répondre aux requêtes récursives demande du temps et des ressources système

Comment configuré un serveur uniquement autoritaire

Arrêter la récursion

- Avec bind9

  options { recursion no ; };

  puis, redémarré named

Vérifier le flag “ra” dans l’en-tête des réponses de votre serveur

dig @196.216.0.X xxxx.cctld.sn soa

Vérifier que votre serveur a la récursion arrêtée

dig @196.216.0.X noc.cctld.sn A

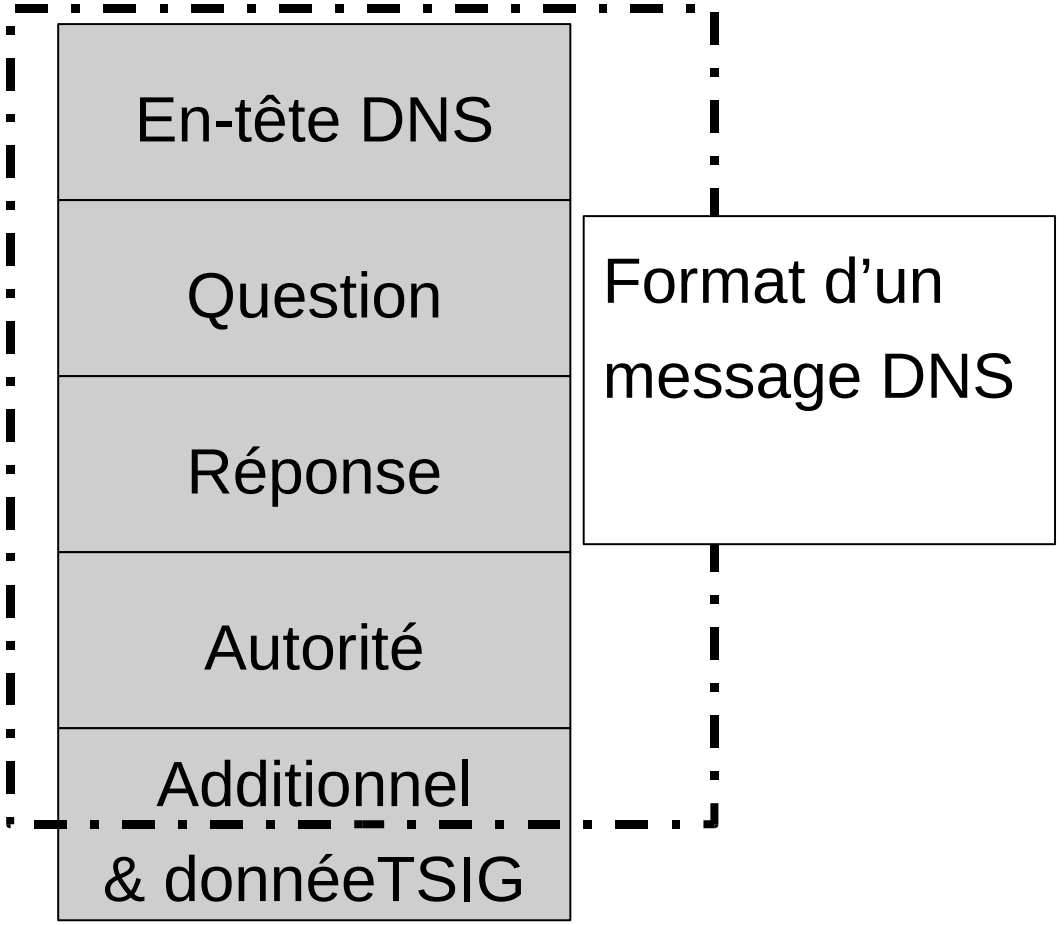
Vous devez avoir une référence vers les serveurs racine

TSIG

Qu’est-ce que TSIG?

- Un mécanisme pour protéger un message d’un resolver au serveur et vice versa
- Un hash avec clé est appliqué(comme une signature digitale). Ainsi le destinataire peut vérifier le message
- Basé sur une valeur secrète partagée – expéditeur et destinataire sont configurés avec la valeur
- RFC2845

TSIG et format des messages



TSIG et format de message

```
;<<>> DiG 9.3.0 <<>> @localhost www.rfi.fr a -k /var/named/keys/Khost1-host2.+157+50032.key

;; QUESTION SECTION:
;www.rfi.fr.                IN      A

;; ANSWER SECTION:
www.rfi.fr.          86400  IN      A       194.117.210.38

;; AUTHORITY SECTION:
rfi.fr.              86400  IN      NS      ns1.mgn.net.
rfi.fr.              86400  IN      NS      ns2.mgn.net.
rfi.fr.              86400  IN      NS      ns3.mgn.net.

;; ADDITIONAL SECTION:
ns1.mgn.net.         172800 IN      A       195.46.193.86
ns2.mgn.net.         172800 IN      A       195.46.193.87
ns3.mgn.net.         172800 IN      A       195.46.214.178

;; TSIG PSEUDOSECTION:
host1-host2.         0      ANY     TSIG    hmac-md5.sig-alg.reg.int. 1126708829 300 16 jfqapw+5tnpqKceNaf5RnQ==
31634 NOERROR 0
```

; <<>> DiG 9.3.0 <<>> @localhost ripe.net a -k /var/named/keys/Khost1-host2.+157+50032.key +dnssec
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;ripe.net. IN A

;; ANSWER SECTION:
ripe.net. 592 IN A 193.0.0.214
ripe.net. 592 IN RRSIG A 5 2 600 20051014125237 20050914125237 49526 ripe.net.
GFWL87C+fcxPkFQ93ifF3SS0eq523Ktv92p0QPGcRs2q4t9pMVy8qjHN oTXEmthamwGdIy90wW5lcUtcfZMTarhx+0Q7zJwO76sXcjjNqMB4nbEb
i2D/596k23DghZ/+Wg/zy/u0yRoYm0LfmbKIZE4WHnb7AeSadKjEz+Ts iuS5wdk5F7SkxginC2JfYRmgxQOQ9NaY

;; ADDITIONAL SECTION:
ripe.net. 3592 IN DNSKEY 257 3 5 AQOTT7bx7N38sPgDWniKnHnSnTxYxdMpEq7dyrDHDaRQgq7DULPWX6ZY
0U1XKKMuNloHRP7H8r17IBhgXcPZjZhtSGYagtPe22mhAMjZ4e8KGgP9 kJTTcpgzoYulvSiETBxjQ42EZWJG+6bxK+vyrwTbqEScmdZfqQz3ltVw
k6Sos0UuSmTeb2C6RSkgHaTpKCu5yIrncVer1gvyvXGv3HOel8jiDGuj 8peNByiaSRD4OIJUxu1jUqLvfDH6Anq6ZeNohxsYVUVajiRl1T+3x5+8
acgwat3V55Z1Nm4O4Z1BKECdPO65EXIEC7/pqs5XvpsiJbafdj03uqLS a3aScpy3
ripe.net. 3592 IN DNSKEY 256 3 5 AQPGmhQPgNllavUXhVoDZZploCWbHr7lqcIGEiR/ct0KCTx4Skp+tBfX
qnq8fz8/UpK4B+s6xIk5FPdjNnFXltdSx81bcM+BadLHL5iuBdQdkH8e yJq2Fk1LAUiP2AB8RAFBd4WQMAklw5z/91jw6aMXSfAo6sSxUFSS1WY8
ChesKvwefNcqglSswlFwxjWHo9XNkFsx0u8=

;; TSIG PSEUDOSECTION:
host1-host2. 0 ANY TSIG hmac-md5.sig-alg.reg.int. 1126710236 300 16 eaDNJtJXavAjVqDZSANllA== 39 NOERROR 0

Nom et valeur secrète

- Nom TSIG
  - Un nom est donné à la clé, le nom est ce qui est transmis dans le message (ainsi le destinataire sait quelle clé l'expéditeur a utilisé)
- Valeur secrète TSIG
  - Une valeur déterminée pendant la production de la clé
  - Généralement codée en Base64
- Ressemble à la clé rndc
  - BIND utilise la même interface pour les clés TSIG et RNDC

Utilisation de TSIG pour protéger AXFR

- Détermination de la valeur secrète
  - `dnssec-keygen -a ... -b ... -n... name`
- Configuration de la clé
  - dans named.conf, même syntaxe que rndc
  - `key { algorithm ...; secret ...;}`
- Utilisation de la clé
  - Dans named.conf
  - `server x { keys ...; }`
  - Où 'x' est l'adresse IP des autres serveurs

Exemple de configuration

Serveur primairer

10.33.40.46

```
key ns1-ns2.zone. {
        algorithm hmac-md5;
        secret "APlaceToBe";
};
server 10.33.40.35 {
        keys {ns1-ns2.zone.;};
};
zone "my.zone.test." {
        type master;
        file...;
        allow-transfer {
                key ns1-ns2.zone.;
                key ns1-ns3.zone.;};
};
```

Serveur secondaire

10.33.40.35

```
key ns1-ns2.zone. {
        algorithm hmac-md5;
        secret "APlaceToBe";
};
server 10.33.40.46 {
  keys {ns1-ns2.zone.;};
};
zone "my.zone.test." {
        type slave;
        file...;
        masters {10.33.40.46;};
        allow-transfer {
                key ns1-ns2.zone.;};
};
```

Une fois encore, la valeur secrète semble ok, mais est invalide

Le temps!!!

- TSIG est sensible au temps – pour arrêter les « attaques de retransmission »
  - La protection des messages expire en 5 minutes
  - S’assurer que les horloges sont synchronisées
  - Pour les tests, régler les horloges
  - En production, un NTP sécurisé est nécessaire

Autres utilisations de TSIG

- TSIG était conçu pour d'autres objectifs
  - Protection des "stub resolvers" sensibles
    - Difficile à réaliser
  - Les mises à jour dynamiques
    - Leur sécurisation dépend du TSIG