Memanfaatkan Split View pada BIND

Catatan singkat ini merupakan over-simplification dari dokumen milik Team Cymru di sini.

Walaupun BIND punya track record jelek dalam masalah keamanannya, namun kita dapat meminimalisasikan resikonya dengan berbagai cara:

- Gunakan chroot
- Manfaatkan fungsi split-view
- Menggunakan DNSSEC/TSIG (tidak dibahas disini)
- Ganti BIND dengan alternatif lainnya (eg. djbdns) :)

Apa yang akan dibahas disini adalah bagaimana mengkonfigurasikan BIND lebih maksimal yang nantinya akan:

- Mengurangi dan menghemat trafik kita ke internet karena hanya akan menjawab recursive query dari jaringan dalam yang lebih dipercaya daripada menjadi “tunggangan” komputer diluar yang memanfaatkan DNS server kita untuk menjawab recursive query (menjadi cache) mereka
- Membatasi atau mengurangi informasi mengenai host-host didalam jaringan diketahui terlalu banyak oleh pihak luar, dengan mencegah AXFR query dan hanya menyediakan informasi atau RR yang diminta (on a need to know basis)

note:

- informasi ini tidak membahas bagaimana mengkonfigurasikan BIND secara mendasar, namun lebih merupakan suatu pelengkap bagaimana mengamankan dan meningkatkan kinerja BIND
- fungsi split-view ini hanya ada di BIND versi 9
- yang dikonfigurasikan disini adalah primary nameserver, walaupun untuk mengkonfigurasikan secondary/slave nameserver cukup memodifikasi beberapa baris saja
- DNSSEC/TSIG tidak dikonfigurasikan disini

Fungsi view pada BIND dapat dimanfaatkan untuk membatasi informasi yang dapat diperoleh dari DNS server, antara informasi yang dapat diperoleh oleh pihak yang dipercaya (trusted/internal) dengan informasi apa yang dapat diperoleh oleh pihak luar (untrusted/external) dapat dibedakan disini

Dengan view ini, kita dapat mengkonfigurasikan supaya BIND menjawab dan meneruskan recursive query yang berasal dari dalam (sekaligus menjadi cache/forwarder jaringan dalam) dan menolak recursive query yang berasal dari pihak luar (hanya menjawab zone/domain dimana DNS server itu ditunjuk sebagai authoritative nameserver), konfigurasi ini sering diabaikan oleh administrator, sehingga menyebabkan DNS server mereka dapat dimanfaatkan oleh pihak luar untuk menjawab recursive query yang bukan authoritative mereka dan secara langsung menggunakan sebagian bandwidth jaringan).

AXFR query atau zone-transfer harus dibatasi hanya kepada nameserver yang berfungsi sebagai secondary/slave atau jaringan internal, deklarasikan melalui access list menjadi:

```
// acl untuk AXFR
acl "xferzone" {
```

```
   // ns2.example.org (secondary ns)
   192.0.34.2;
};
```

Network yang dapat melakukan recursive query dideklarasikan melalui :

```
// acl untuk internal/trusted network
acl "trusted" {
   192.0.34.0/24;
   202.155.0.0/24;
};
```

Berikutnya pada “option” kita dapat mendeklarasikan:

```
option {
   // allow axfr only to secondary nameservers
   zone-transfer "xferzone";

   // allow only trusted/internal network to do recursive query
   allow-query "trusted";
};
```

Untuk mendeklarasikan view, gunakan keyword view pada file named.conf:

```
// view for internal trusted networks
view "internal-net" in {
   match-clients { trusted; };
   recursion yes;

   // begin zone declarations

   zone "." in {
      type "hint";
      file "named.ca";
   };

   zone "0.0.127.in-addr.arpa." in {
      type "master";
      file "master/db.0.0.127.in-addr.arpa";
   };

   // include another zone
   include "named-db.conf";
}

// view for external untrusted networks
view "untrusted" in {
   match-client { any; };
   recursion no;

   additional-from-auth no;
```

```
   additional-from-cache no;

   zone "." IN {
    type hint;
    file "named.ca";
   };

   include "named-db.conf";
};
```

zone yang authoritative akan diletakkan di file tersendiri (named-db.conf):

```
zone "example.org." {
   type master;
   file "master/db.example.org";
};

zone "34.0.192.in-addr.arpa" {
   type master;
   file "master/db.34.0.192.in-addr.arpa";
};
```

Sehingga isi named.conf kira-kira akan seperti ini:

```
// acl untuk AXFR
acl "xferzone" {
   // ns2.example.org (secondary ns)
   192.0.34.2;
};

// acl untuk internal/trusted network
acl "trusted" {
   192.0.34.0/24;
   202.155.0.0/24;
};

option {
   // allow axfr only to secondary nameservers
   zone-transfer "xferzone";

   // allow only trusted/internal network to do recursive query
   allow-query "trusted";
};

// view for internal trusted networks
view "internal-net" in {
   match-clients { trusted; };
   recursion yes;

   // begin zone declarations
```

```
   zone "." in {
      type "hint";
      file "named.ca";
   };

   zone "0.0.127.in-addr.arpa." in {
      type "master";
      file "master/db.0.0.127.in-addr.arpa";
   };

   // include another zone
   include "named-db.conf";
}

// view for external untrusted networks
view "external-net" in {
   match-client { any; };
   recursion no;

   additional-from-auth no;
   additional-from-cache no;

   zone "." IN {
    type hint;
    file "named.ca";
   };

   include "named-db.conf";
};

zone "example.org." {
   type master;
   file "master/db.example.org";
};

zone "34.0.192.in-addr.arpa" {
   type master;
   file "master/db.34.0.192.in-addr.arpa";
};
```

Referensi:

- [[http://www.cymru.com/Documents/secure-bind-template.html | Secure BIND Template]
- [http://www.layangan.com/asfik/writings/dns-bind.html | Konsep dan konfigurasi BIND oleh Asfik]