

Written by Ogeb
Monday, 05 March 2007 21:23

PERHATIAN:

1. Jangan pernah mencoba ini jika anda tidak tau apa yang anda lakukan.
2. Jangan pula mencoba ini jika anda tidak tau apa itu FreeBSD dan anda tidak tau serta tidak mengerti perintah-perintah *nix variant.
3. Siapkan rokok + kopi secukupnya jika anda perokok berat, karena proses ini akan memakan waktu.
4. Tulisan ini didedikasikan untuk kemajuan FreeBSD di Indonesia.
5. Silakan mengcopy atau memperbanyak tulisan ini tanpa seijin saya demi kemajuan FreeBSD di Indonesia.

Tulisan ini berawal dari keisengan saya yang ingin membuat server saya menjadi lebih optimal dan lebih terhindar dari hal-hal yang tidak diinginkan. Awalnya saya ingin membuat sebuah NS server menggunakan Bind untuk domain baru saya, setelah instalasi selesai lalu saya mencoba mencheek hasil dari konfigurasi saya pada

<http://dnsreport.com/tools/dnsreport.ch?domain=a.isplud.net>

Walhasil pada baris ke 5, ada warna merah dengan huruf **KAPITAL** bertuliskan FAIL Open DNS servers dan ada keterangan di sebelah kanannya.

"ERROR: One or more of your nameservers reports that it is an open DNS server. This usually means that anyone in the world can query it for domains it is not authoritative for (it is possible that the DNS server advertises that it does recursive lookups when it does not, but that shouldn't happen). This can cause an excessive load on your DNS server. Also, it is strongly discouraged to have a DNS server be both authoritative for your domain and be recursive (even if it is not open), due to the potential for cache poisoning (with no recursion, there is no cache, and it is impossible to poison it). Also, the bad guys could use your DNS server as part of an attack, by forging their IP address. Problem record(s) are: ..."

Hmm... saya kira awalnya bind yang saya install telah benar-benar secure, selain jailed pada version juga saya hide menjadi "Tong noong Goblok", setelah mendapat tulisan error di atas, akhirnya saya berpikir, wah kalo demikian NS saya masih kayak jalan tol blas... blas... tinggal tunggu waktu aja ada yang query rame-rame akan terjadi hal-hal yang tidak diinginkan. Ok, kita sudah saja omong kosong yang tidak berguna ini, mari kita lanjutkan ke tahap berikutnya yaitu instalasi Bind.

```
#cd /usr/ports/dns/bind9
```

```
#make ; make install
```

Written by Ogeb

Monday, 05 March 2007 21:23

Jrenggg... beres dah proses instalasi. Betapa nikmatnya menggunakan FreeBSD ini, tahap selanjutnya mengkonfigurasi.

Acuan konfigurasi yang saya gunakan merujuk ke situs <http://www.cymru.com/Documents/secure-bind-template.html>, lalu disesuaikan dengan konfigurasi network saya.

```
# cd /etc/namedb
# pico named.conf
```

```
-----isi file named.conf-----
```

```
// @(#)named.conf 02 OCT 2001 Rob Thomas robt@cymru.com
// Set up our ACLs
// In BIND 8, ACL names with quotes were treated as different from
// the same name without quotes. In BIND 9, both are treated as
// the same.
```

```
acl "xfer" {
    69.94.133.163; // Allow no transfers. If we have other
    // name servers, place them here.
    // Note that in the Netherlands, for example,
    // the TLD servers 193.176.144.2, 194.53.253.100, and 193.176.144.128/28
    // are allowed to perform zone tranfers from the domains under.nl. The
    // RIPE NCC had requested in the past that reverse (in-addr.arpa) zones
    // permit zone transfer requests from 193.0.0.0/23.
```

```
};
```

```
acl "trusted" {
    // Place our internal and DMZ subnets in here so that
    // intranet and DMZ clients may send DNS queries. This
    // also prevents outside hosts from using our name server
    // as a resolver for other domains.
    localhost;
```

```
};
```

```
acl "bogon" {
    // Filter out the bogon networks. These are networks
    // listed by IANA as test, RFC1918, Multicast, experi-
    // mental, etc. If you see DNS queries or updates with
    // a source address within these networks, this is likely
    // of malicious origin. CAUTION: If you are using RFC1918
    // netblocks on your network, remove those netblocks from
    // this list of blackhole ACLs!
    0.0.0.0/8;
```

Written by Ogeb

Monday, 05 March 2007 21:23

1.0.0.0/8;
2.0.0.0/8;
5.0.0.0/8;
7.0.0.0/8;
10.0.0.0/8;
7.0.0.0/8;
10.0.0.0/8;
23.0.0.0/8;
27.0.0.0/8;
31.0.0.0/8;
36.0.0.0/8;
37.0.0.0/8;
39.0.0.0/8;
42.0.0.0/8;
49.0.0.0/8;
50.0.0.0/8;
77.0.0.0/8;
78.0.0.0/8;
79.0.0.0/8;
92.0.0.0/8;
93.0.0.0/8;
94.0.0.0/8;
95.0.0.0/8;
96.0.0.0/8;
97.0.0.0/8;
98.0.0.0/8;
99.0.0.0/8;
100.0.0.0/8;
101.0.0.0/8;
102.0.0.0/8;
103.0.0.0/8;
104.0.0.0/8;
105.0.0.0/8;
106.0.0.0/8;
107.0.0.0/8;
108.0.0.0/8;
109.0.0.0/8;
110.0.0.0/8;
111.0.0.0/8;
112.0.0.0/8;
113.0.0.0/8;
114.0.0.0/8;
115.0.0.0/8;
116.0.0.0/8;
117.0.0.0/8;
116.0.0.0/8;

Written by Ogeb

Monday, 05 March 2007 21:23

```
117.0.0.0/8;
118.0.0.0/8;
119.0.0.0/8;
120.0.0.0/8;
169.254.0.0/16;
172.16.0.0/12;
173.0.0.0/8;
174.0.0.0/8;
175.0.0.0/8;
176.0.0.0/8;
177.0.0.0/8;
178.0.0.0/8;
179.0.0.0/8;
180.0.0.0/8;
181.0.0.0/8;
182.0.0.0/8;
183.0.0.0/8;
184.0.0.0/8;
185.0.0.0/8;
186.0.0.0/8;
187.0.0.0/8;
192.0.2.0/24;
192.168.0.0/16;
197.0.0.0/8;
223.0.0.0/8;
224.0.0.0/3;
};

logging {
    channel default_syslog {
        // Send most of the named messages to syslog.
        syslog local2;
        severity debug;
    };

    channel audit_log {
        // Send the security related messages to a separate file.
        file &quot;/etc/namedb/log/log&quot;;
        severity debug;
        print-time yes;
    };

    category default { default_syslog; };
    category general { default_syslog; };
    category security { audit_log; default_syslog; };
    category config { default_syslog; };
};
```

Written by Ogeb

Monday, 05 March 2007 21:23

```
category resolver { audit_log; };
category xfer-in { audit_log; };
category xfer-out { audit_log; };
category notify { audit_log; };
category client { audit_log; };
category network { audit_log; };
category update { audit_log; };
category queries { audit_log; };
category lame-servers { audit_log; };

};
// Set options for security

options {

    directory &quot;/etc/namedb&quot;;
    pid-file &quot;/var/run/named/pid&quot;;
    statistics-file &quot;/var/stats/named.stats&quot;;
    memstatistics-file &quot;/var/stats/named.memstats&quot;;
    dump-file &quot;/var/dump/named_dump.db&quot;;
    zone-statistics yes;
    listen-on { 127.0.0.1; 192.168.1.254 ; 202.153.240.1 ; 202.159.32.2 ; 202.159.33.2 ; };

    // Prevent DoS attacks by generating bogus zone transfer
    // Prevent DoS attacks by generating bogus zone transfer
    // requests. This will result in slower updates to the
    // slave servers (e.g. they will await the poll interval
    // before checking for updates).

    notify no;

    // Generate more efficient zone transfers. This will place
    // multiple DNS records in a DNS message, instead of one per
    // DNS message.

    transfer-format many-answers;
    // Set the maximum zone transfer time to something more
    // reasonable. In this case, we state that any zone transfer
    // that takes longer than 60 minutes is unlikely to ever
    // complete. WARNING: If you have very large zone files,
    // adjust this to fit your requirements.

    max-transfer-time-in 60;

    // We have no dynamic interfaces, so BIND shouldn't need to
    // poll for interface state {UP|DOWN}.
```

Written by Ogeb

Monday, 05 March 2007 21:23

```
interface-interval 0;

allow-transfer {
    // Zone transfers limited to members of the
    // "xfer" ACL.
    xfer;
};

allow-query {
    // Accept queries from our "trusted" ACL. We will
    // allow anyone to query our master zones below.
    // This prevents us from becoming a free DNS server
    // to the masses.

    trusted;
};

blackhole {
    // Deny anything from the bogon networks as
    // detailed in the "bogon" ACL.
    bogon;
};

view "internal-in" in {
    // Our internal (trusted) view. We permit the internal networks
    // to freely access this view. We perform recursion for our
    // internal hosts, and retrieve data from the cache for them.
    match-clients { trusted; };
    recursion yes;
    additional-from-auth yes;
    additional-from-cache yes;

    zone "." in {
        type hint;
        file "db.cache";
    };

    zone "0.0.127.in-addr.arpa" in {
        // Allow queries for the 127/8 network, but not zone transfers.
        // Every name server, both slave and master, will be a master
        // for this zone.
        type master;
        file "master/db.127.0.0";
    };
};
```

Written by Ogeb

Monday, 05 March 2007 21:23

```
    allow-query { any; };
    allow-transfer { none; };
};

// Create a view for external DNS clients.

view "external-in" in {
    // Our external (untrusted) view. We permit any client to access
    // portions of this view. We do not perform recursion or cache
    // access for hosts using this view.

    match-clients { any; };
    recursion no;
    additional-from-auth no;
    additional-from-cache no;

    // Link in our zones

    zone "." in {
        type hint;
        file "db.cache";
    };

    zone "a.isplud.net" in {
        type master;
        file "master/db.a.isplud.net";
        allow-query { any; };
    };

    zone "12.252.66.in-addr.arpa" {
        type master;
        file "master/db.ip";
        allow-query { any; };
    };
};

view "external-chaos" chaos {
    match-clients { any; };
    recursion no;

    zone "." {
        type hint;
        file "/dev/null";
    };

    zone "bind" {
```

Written by Ogeb

Monday, 05 March 2007 21:23

```
    type master;
    file "master/db.bind";
    allow-query { trusted; };
    allow-transfer { none; };
};
};
```

-----isi file named.conf-----

buat file db.cache yang isinya adalah named.root

```
# cp named.root db.cache
```

lalu buat db.bind zonefile

```
@(#)db.bind v1.2 25 JAN 2001 Rob Thomas robt@cymru.com;
    $TTL 1D
    $ORIGIN bind.
@ 1D CHAOS SOA localhost. root.localhost. (
    2001013101 ; serial
    3H ; refresh
    1H ; retry
    1W ; expiry
    1D ) ; minimum
```

```
CHAOS NS localhost.
```

```
version.bind. CHAOS TXT "BIND 9.1.3+robhacks";
```

```
authors.bind. CHAOS TXT "are better coders than I.:";
```

selanjutnya buat zone yang lain nya yaitu xone domain saya

```
#pico db.a.isplud.net
```

```
$TTL 86400
$ORIGIN a.isplud.net.
@ IN SOA aztech.a.isplud.net. ogb.indofreebsd.or.id. (
    2006031307; serial
    28800
    7200
    1209600
    86400
)
```

```
IN NS aztech.a.isplud.net.
```

```
IN NS zerg.a.isplud.net.
```

```
IN NS athena.a.isplud.net.
```

Written by Ogeb

Monday, 05 March 2007 21:23

```
IN NS zeus.a.isplud.net.  
IN NS ns2.afraid.org.  
IN A 66.252.12.50
```

```
$ORIGIN a.isplud.net.  
aztech IN A 66.252.12.50  
zerg IN A 66.252.12.51  
athena IN A 66.252.12.2  
zeus IN A 66.252.12.3  
admin IN A 66.252.12.125  
razor.cybertech IN A 66.252.12.126
```

membuat file zone ptr

```
#pico db.ip  
$ORIGIN.  
$TTL 3600 ; 1 hour  
12.252.66.in-addr.arpa IN SOA aztech.a.isplud.net. ogb@indofreebsd.or.id. (  
    2006032023;  
    28800  
    14400  
    3600000  
    86400  
)
```

```
IN NS aztech.a.isplud.net.  
IN NS zerg.a.isplud.net.  
IN NS athena.a.isplud.net.  
IN NS zeus.a.isplud.net.
```

```
$ORIGIN 12.252.66.in-addr.arpa.  
125 IN PTR admin.a.isplud.net.  
126 IN PTR razor.cybertech.a.isplud.net.
```

nah sampe di sini selesailah kita membuat sebuah DNS server yang secure versi <http://www.cymru.com/Documents/secure-bind-template.html>

Maaf bila ada kekurangan pada tulisan ini yang semata-mata karena keterbatasan pengetahuan saya dan keterbatasan waktu saya untuk mengexplore lebih jauh tentang bind security.

Akhir kata saya ucapkan banyak terima kasih kepada semua teman saya di #indofreebsd irc.dal.net