# How to block or sinkhole domains in BIND

There may come a time when you may require to sinkhole or block some domains.

One of the easiest way of doing this is within your DNS infrastructure by making your DNS Resolvers authoritative for the domains that you wish to block.

Within your BIND configuration file which on Debian based systems is normally located at /etc/bind/named.conf.local you will need to specify which domains you want to block.

***named.conf.local***

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

include "/etc/bind/blacklisted.zones";

zone "example.local" {
       type master;
       file "/etc/bind/zones/master/example.local.db";
};
```

In the example named.conf.local configuration file above the line stating to include *"/etc/bind/blacklisted.zones".* Within this file we are going to define the domains that we want to block or sinkhole. We purposely avoid placing the domains we want to block or sink hole in named.conf.local by including another file for ease of configuration and updating.

***blacklisted.zones***

```
zone "blockeddomain.com" {type master?; file
"/etc/bind/zones/master/blockeddomains.db";};
zone "buymalwarehere.ru" {type master; ?file
"/etc/bind/zones/master/blockeddomains.db";};
zone "s23a93884skf.net" {type master; file
"/etc/bind/zones/master/blockeddomains.db";};
zone "almost-somedodgeybank.com" {type master; file
"/etc/bind/zones/master/blockeddomains.db";};
zone "google.co.uk" {type master; file
"/etc/bind/zones/master/blockeddomains.db";};
```

As you can see above we are defining the zones that you are authoritative for. When a query is received by the DNS server for baddomain.com the server will provide data from the associated file. In this case as we are treating all of these as sink holed domains they can all

point to the same zone file again for ease of use.

***blockeddomains.db***

```
;
; BIND data file for example.local
;
$TTL    3600
@       IN      SOA     ns1.example.local. info.example.local. (
                            2014052101         ; Serial
                                 7200         ; Refresh
                                  120         ; Retry
                               2419200         ; Expire
                                  3600)        ; Default TTL
;
                A       192.168.56.200 ; This means that
naughydomain.com gets directed to the designated address
*       IN      A       192.168.56.200 ; This wildcard entry means
that any permutation of xxx.naughtydomain.com gets directed to the
designated address
                AAAA    ::1 ; This means that naughydomain.com gets
directed to IPv6 localhost
*       IN      AAAA    ::1 ; This wildcard entry means that any
permutation of xxx.naughtydomain.com gets directed to IPv6 localhost
```

The records in the zone file will point any of the domains that use this definition to 192.168.56.200 or ::1. In this case, this is to a specific IP address where connections to it are monitored in order to generate information about the connections. If you wanted to block the connections you would just Change this to 127.0.0.1

Once all of the configuration changes above are complete you need to reload/reconfigure your DNS server

Now your internal resolver will be authoritative for all of the domains that were listed in the blacklisted.zones, as such lets give this a test.

Shown below the output of a lookup for www.google.co.uk [1] before making any configuration changes.

```
~$ dig @192.168.56.101 www.google.co.uk

; <<>> DiG 9.8.1-P1 <<>> @192.168.56.101 www.google.co.uk
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29972
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
;www.google.co.uk. IN A
```

```
;; ANSWER SECTION:
www.google.co.uk. 300 IN A 173.194.34.120
www.google.co.uk. 300 IN A 173.194.34.127
www.google.co.uk. 300 IN A 173.194.34.119

;; AUTHORITY SECTION:
google.co.uk. 172800 IN NS ns4.google.com.
google.co.uk. 172800 IN NS ns2.google.com.
google.co.uk. 172800 IN NS ns1.google.com.
google.co.uk. 172800 IN NS ns3.google.com.

;; Query time: 48 msec
;; SERVER: 192.168.56.101#53(192.168.56.101)
;; WHEN: Wed May 21 10:55:28 2014
;; MSG SIZE  rcvd: 164
```

We can now see that the changes have taken effect as the results of the query is to the sinkhole IP.

```
~$ dig @192.168.56.101 www.google.co.uk

; <<>> DiG 9.8.1-P1 <<>> @192.168.56.101 www.google.co.uk
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44103
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2,
ADDITIONAL: 2

;; QUESTION SECTION:
;www.google.co.uk. IN A

;; ANSWER SECTION:
www.google.co.uk. 604800 IN A 192.168.56.200

;; AUTHORITY SECTION:
google.co.uk. 604800 IN NS ns1.example.local.
;; ADDITIONAL SECTION:

ns1.example.local. 604800 IN A 192.168.56.101
;; Query time: 20 msec

;; SERVER: 192.168.56.101#53(192.168.56.101)
;; WHEN: Wed May 21 11:07:29 2014
;; MSG SIZE  rcvd: 131
```

As we can see from the return of the above query the domain google.co.uk, which was defined within the blacklisted.zones, is now being directed to 192.168.56.200

```
~$dig @192.168.56.101 gobledegoook.google.co.uk

; <<>> DiG 9.8.1-P1 <<>> @192.168.56.101 gobledegoook.google.co.uk
; (1 server found)
```

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13427
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 1

;; QUESTION SECTION:
;gobledegoook.google.co.uk. IN A

;; ANSWER SECTION:
gobledegoook.google.co.uk. 3600 IN A 192.168.56.200

;; AUTHORITY SECTION:
google.co.uk. 3600 IN NS ns1.example.local.

;; ADDITIONAL SECTION:
ns1.example.local. 604800 IN A 192.168.56.101

;; Query time: 0 msec
;; SERVER: 192.168.56.101#53(192.168.56.101)
;; WHEN: Wed May 21 15:18:48 2014
;; MSG SIZE  rcvd: 106
```

As we can see from the return of the above query the domain gobledegoook.google.co.uk as it is part of the wild card entry of google.co.uk means that any sub domains of google.co.uk will be blocked or redirected to the IP of your choosing.

## Caveats to blocking domains

There are some easy ways that clients may be able to mitigate these DNS configurations. By modifying their hosts file on their systems to point at the correct IP addresses for the domains or by using a public resolver however both of these methods will require local administrator access.

You should only do this on your internal resolvers, if you take these actions on your public facing authoritative servers then you will be responding to domains which are not your responsibility.

Taking these actions on domains which are secured with DNSSEC will also break the security on them. If validation is turned on then the resolution will fail and the sinkhole will not get contacted.

Since BIND 9.8.1 you can build a DNS firewalls with (RPZ) information on this is available from https://deepthought.isc.org/article/AA-00525/110/Building-DNS-Firewalls-with-Response-Policy-Zones-RPZ.html [2]

---



**Links**
[1] http://www.google.co.uk
[2] https://deepthought.isc.org/article/AA-00525/110/Building-DNS-Firewalls-with-Response-Policy-Zones-

RPZ.html