STEALTH (A.K.A. DMZ OR HIDDEN MASTER) NAME SERVER

A stealth server is defined as being a name server which does not appear in any **publicly visible** NS Records for the domain. The stealth server can be roughly defined as having the following characteristics:

1. The organisation needs a public DNS to enable access to its public services e.g. web, mail ftp etc..
2. The organisation does not want the world to see any of its internal hosts either by interrogation (query or zone transfer) or should the DNS service be compromised.

A Stealth configuration is shown in Figure 4-5.

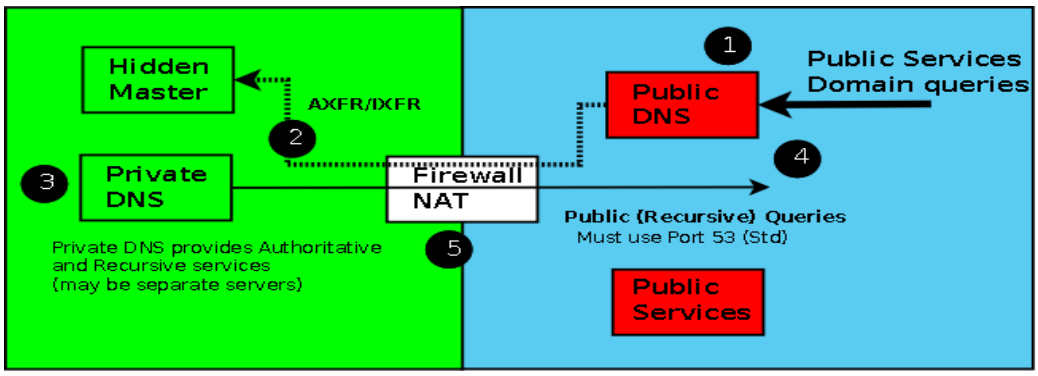

Figure 4-5 Stealth Server Topology

The external server(s) is(are) configured to provide Authoritative Only responses and no caching (no recursive queries accepted). The zone file for this server would be unique and would contain ONLY those systems or services that are publicly visible e.g. SOA, NS records for the public (not stealth) name servers, MX record(s) for mail servers and www and ftp service A records. Zone transfers can be allowed between the public servers as required but they MUST NOT transfer or accept transfers from the Stealth server. While this may seem to create more work, the concern is that should the host running the external service be compromised then inspection of the named.conf or zone files must provide no more information than is already publically visible. If 'master', 'allow-notify','allow-transfer' options are present in named.conf (each of which will contain a private IP) then the attacker has gained more knowledge about the organisation - they have penetrated the 'veil of privacy'.

There are a number of articles which suggest that the view statement may be used to provide similar functionality using a single server but this does not address the problem of the DNS host system being compromised and by simple inspection of the named.conf file additional data about the organisation could be discovered. In our opinion 'view' does not provide adequate security in a 'Split DNS' solution.

A minimal public zone file is shown below:

```
; public zone master file
; provides minimal public visibility of external services
example.com.  IN      SOA    ns.example.com. root.example.com. (
                        2003080800 ; se = serial number
                        3h         ; ref = refresh
                        15m        ; ret = update retry
                        3w         ; ex = expiry
                        3h      ; min = minimum
                        )
            IN      NS      ns1.example.com.
            IN      NS      ns2.example.com.
            IN      MX  10  mail.example.com.
ns1           IN      A       192.168.254.1
ns2           IN      A       192.168.254.2
mail          IN      A       192.168.254.3
www           IN      A       192.168.254.4
ftp           IN      A       192.168.254.5
```

The internal server (the Stealth Server) can be configured to make visible internal and external services, provide recursive queries and all manner of other services. This server would use a private zone master file which could look like this:

```
; private zone master file used by stealth server(s)
; provides public and private services and hosts
example.com.  IN      SOA    ns.example.com. root.example.com. (
                        2003080800 ; se = serial number
                        3h         ; ref = refresh
                        15m        ; ret = update retry
                        3w         ; ex = expiry
                        3h         ; min = minimum
                        )
            IN      NS      ns1.example.com.
            IN      NS      ns2.example.com.
            IN      MX  10  mail.example.com.
; public hosts
ns1           IN      A       192.168.254.1
ns2           IN      A       192.168.254.2
mail          IN      A       192.168.254.3
www           IN      A       192.168.254.4
```

```
ftp          IN      A       192.168.254.5

; private hosts

joe          IN      A       192.168.254.6

bill         IN      A       192.168.254.7

fred         IN      A       192.168.254.8

....

accounting   IN      A       192.168.254.28

payroll      IN      A       192.168.254.29
```

Using BIND 9's view statement can provide different services to internal and external requests can reduce further the Stealth server's visibility e.g. forwarding all DNS internal requests to the external server.

Source: http://www.zytrax.com/books/dns/ch4/