DNS for Internet Firewalls

1

DNS Security

- Do not rely on DNS names to make security-related decisions
  - DNS can be spoofed
- Use IP addresses whenever possible
  - Note that IP addresses can ***also*** be spoofed
  - It's just a little harder

2

DNS Hiding

- Hiding DNS does not improve security
  - It is very easy to learn about a network once you've penetrated it
  - Many other ways for host/address information to leak out
- Hiding DNS may be necessary if you do not have valid IP addresses
  - Or many unreachable nodes/networks

3

Futility of DNS Hiding *(cont)*

```
% ping -s 192.239.76.255
PING 192.239.76.255: 56 data bytes
64 bytes from dev.gdb.org (192.239.76.2): icmp_seq=0. time=17.
   ms
64 bytes from crab.gdb.org (192.239.76.190): icmp_seq=0.
   time=47. ms
64 bytes from screams.gdb.org (192.239.76.6): icmp_seq=0.
   time=56. ms
64 bytes from hamlet.gdb.org (192.239.76.134): icmp_seq=0.
   time=69. ms
64 bytes from thor.gdb.org (192.239.76.47): icmp_seq=0.
   time=73. ms
64 bytes from oscar.gdb.org (192.239.76.36): icmp_seq=0.
   time=78. ms
...
```

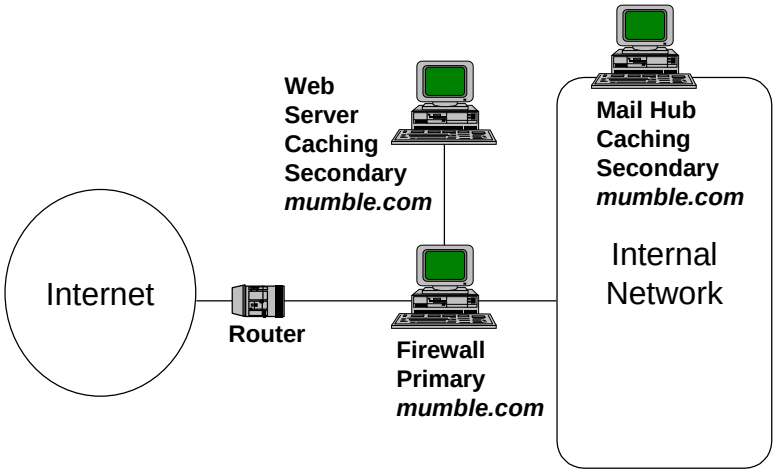
4

Futility of DNS Hiding *(cont)*

```
From ches@plan9.bell-labs.com Wed Mar 20 17:32 EST 1996
Received: from smartwall.v-one.com (firewall-user@smartwall.v-one.com
   [206.205.74.11]) by mail.Clark.Net (8.7.3/8.6.5) with SMTP id
   RAA08728 for <mjr@clark.net> ; Wed, 20 Mar 1996 17:32:48 -0500 (EST)
Received: by smartwall.v-one.com; id RAA01262; Wed, 20 Mar 1996
   17:28:29 -0500
Received: from smartwall.v-one.com (firewall-user@smartwall-internal.v-
   one.com [198.69.135.11]) by uxdev2.v-one.com (8.6.5/8.6.5) with
   ESMTP id RAA03713 for <mjr@v-one.com>; Wed, 20 Mar 1996 17:42:50 -
   0500
Received: by smartwall.v-one.com; id RAA01253; Wed, 20 Mar 1996
   17:28:18 -0500 X-UIDL: 827720348.002
From: ches@plan9.bell-labs.com
...
```

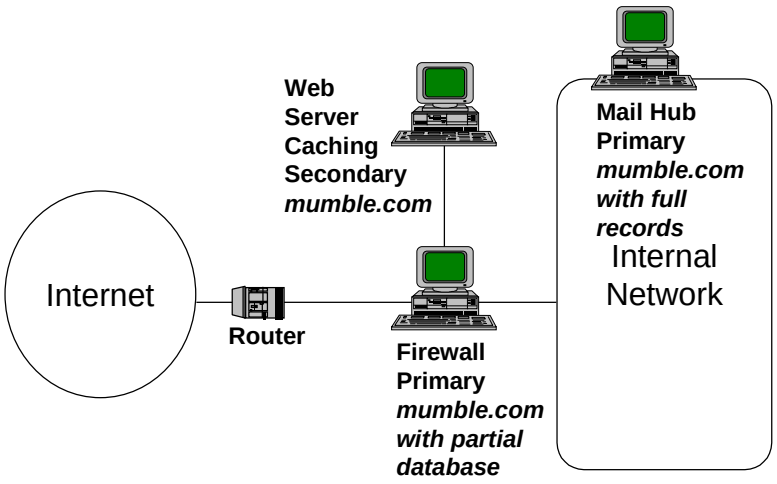
5

Typical DNS Environment



6

Hidden DNS Environment



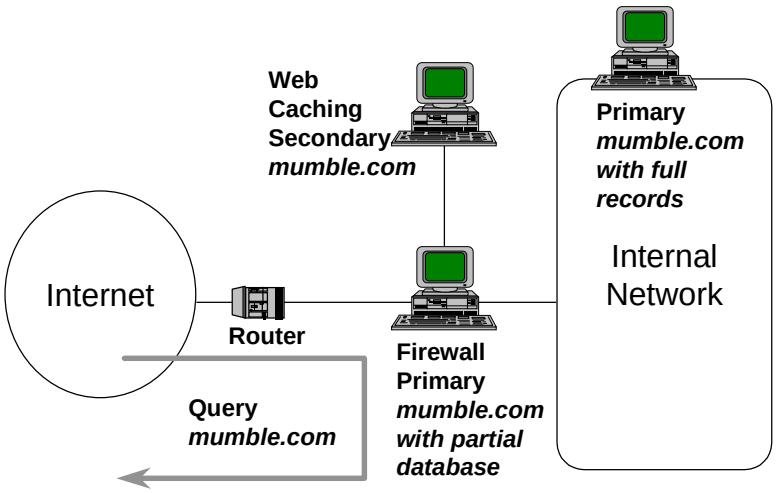
7

warninG!!

- The following is a really warped solution
  - "As ugly as a 2-week old pepperoni pizza" (Paul Vixie)
- Use it only if you are not willing to maintain two separate dns databases on the firewall

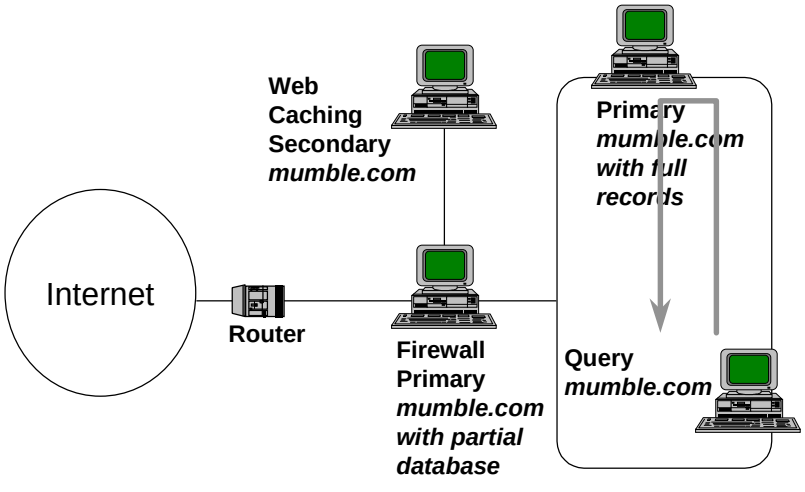
8

External Queries



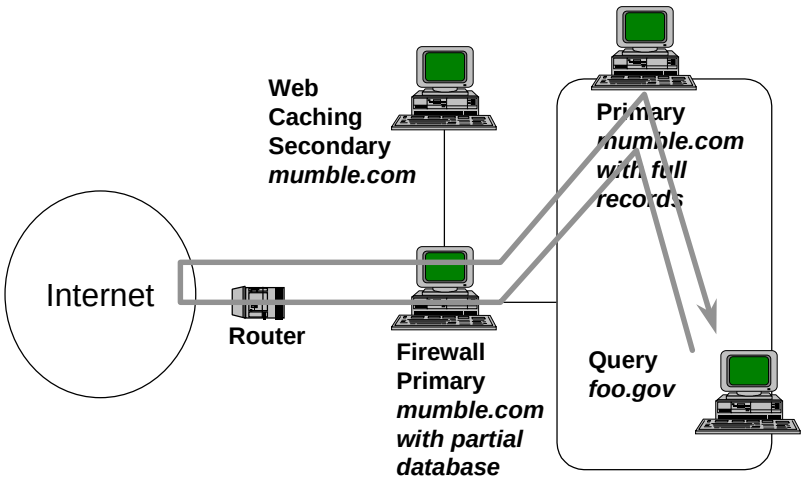
9

Internal->Internal Queries



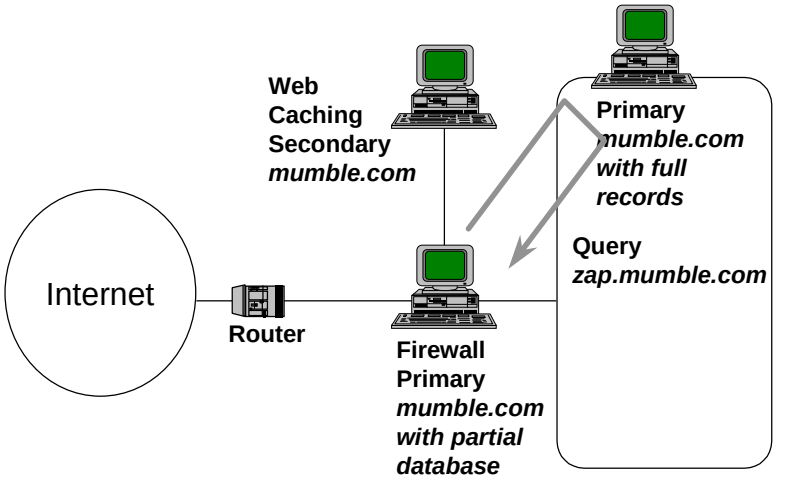
10

Internal->External Queries



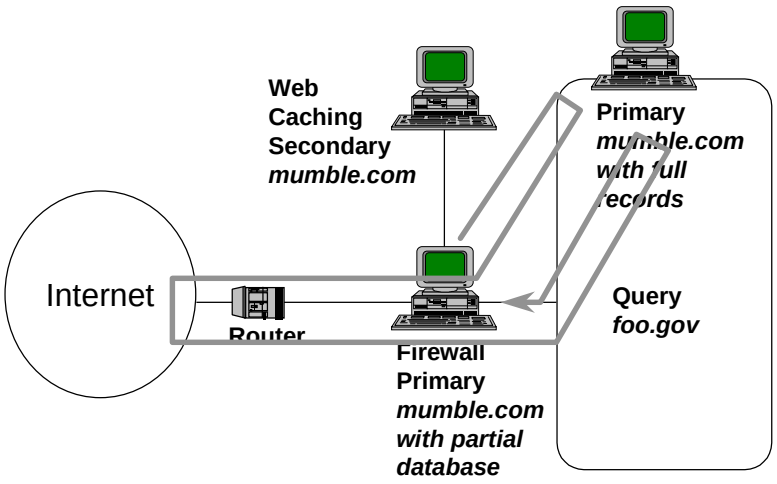
11

Firewall->Internal Queries



12

Firewall->External Queries



13

DNS Config on Firewall

- Primary for domain
- Resolv.conf points to *internal* nameserver

```
domain          mumble.com
nameserver      168.143.0.7
```

14

DNS on Inside Nameserver

- Named.boot has “forwarders” record
- All unsolved queries go to firewall

```
cache           .               /etc/named.ca
primary mumble.com              /etc/named.mumble
primary 76.239.192.in-addr.arpa /etc/named.mumble.76
primary 77.239.192.in-addr.arpa /etc/named.mumble.77

slave                     ; do not contact outside directly
forwarders   192.239.76.1 ; the firewall

primary         0.0.127.in-addr.arpa    /etc/named.local
```

15