Frobbit!

DEPLOYING DNS IN THE ENTERPRISE

Patrik Fältström

DEPLOYING DNS IN THE ENTERPRISE

Patrik Fältström

Office of the CTO

måndag 3 november 2008

This is what the DNS is for

- Translation of domain name to IPv4 address

```
www.example.com. IN A 192.168.1.1
```

- Translation of domain name to IPv6 address

```
www.example.com. IN AAAA 2001:1670:b87:4:207:e9ff:fe1b:5c09
```

- Lookup of mail server given mail domain

```
example.com. IN MX 10 mail.example.com.
```

- Translation of IPv4 address to domain name

```
1.1.168.192.in-addr.arpa. IN PTR www.example.com.
```

- Lookup host and port for services

```
_sip._tcp.example.com. IN SRV 0 10 5060 sip.example.com.
```

- Lookup of service given domain name

```
example.com. IN NAPTR 1 1 "s" "" "" _sip._tcp.example.com.
```

- Lookup of URL’s given E.164 number

```
5.4.3.2.1.e164.arpa. IN NAPTR 1 1 "u" "E2U+sip" "!.*!sip:joe@example.com!" .
```

Queries

- Lookup is based on name, class and type

Query for cisco.com:

example.com.	?	IN	A	?

Get back the answer 198.133.219.25:

example.com.	4711	IN	A	198.133.219.25

Domains and Zones

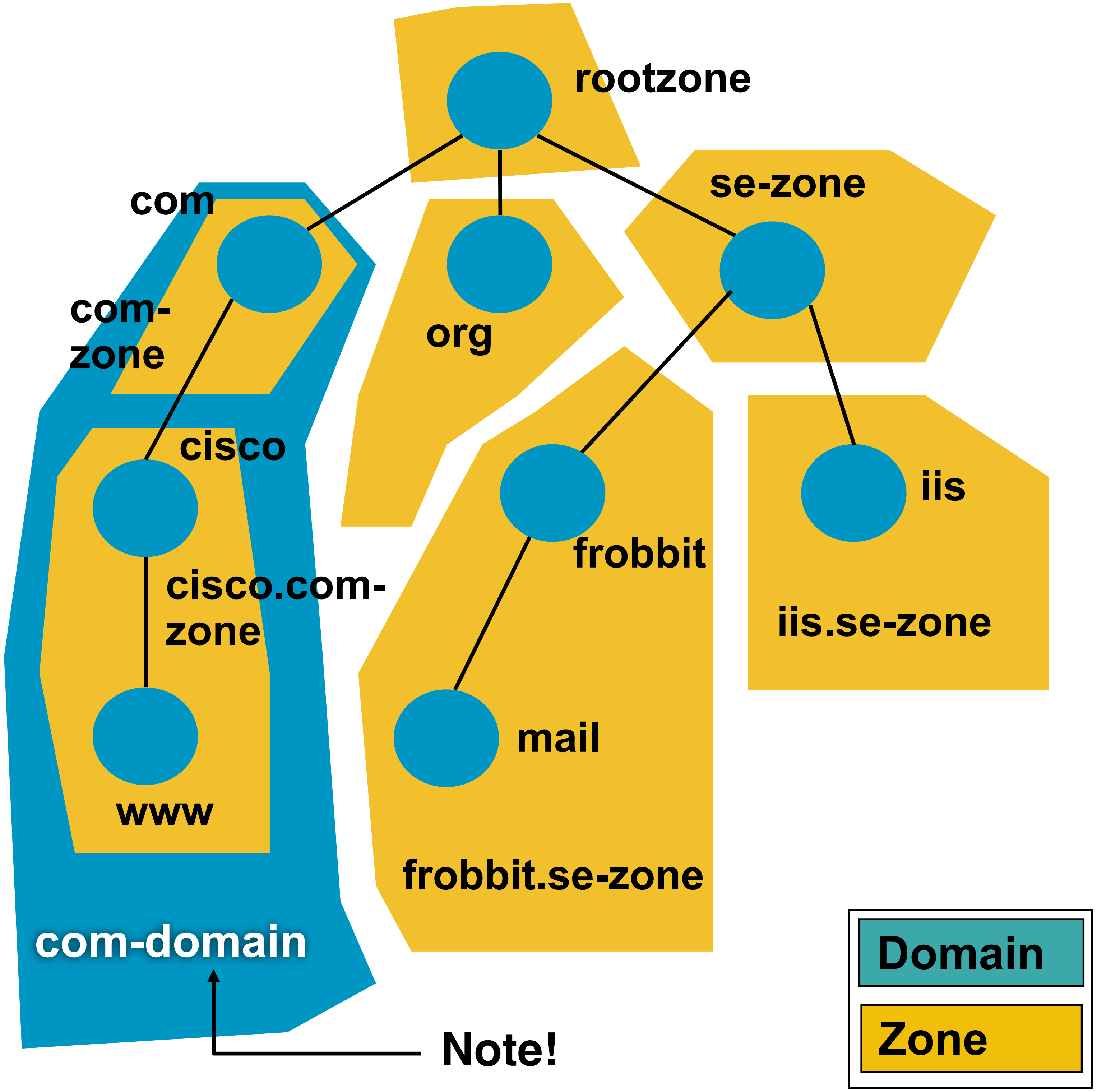
- Nodes/tokens are grouped in “zones”

  Each zone is an administrative unit

  Each node can be the start of a new zone, but it doesn’t have to be

  A node which is the start of a new zone is called a “delegation point”

- All nodes below a node are included in the same “domain”



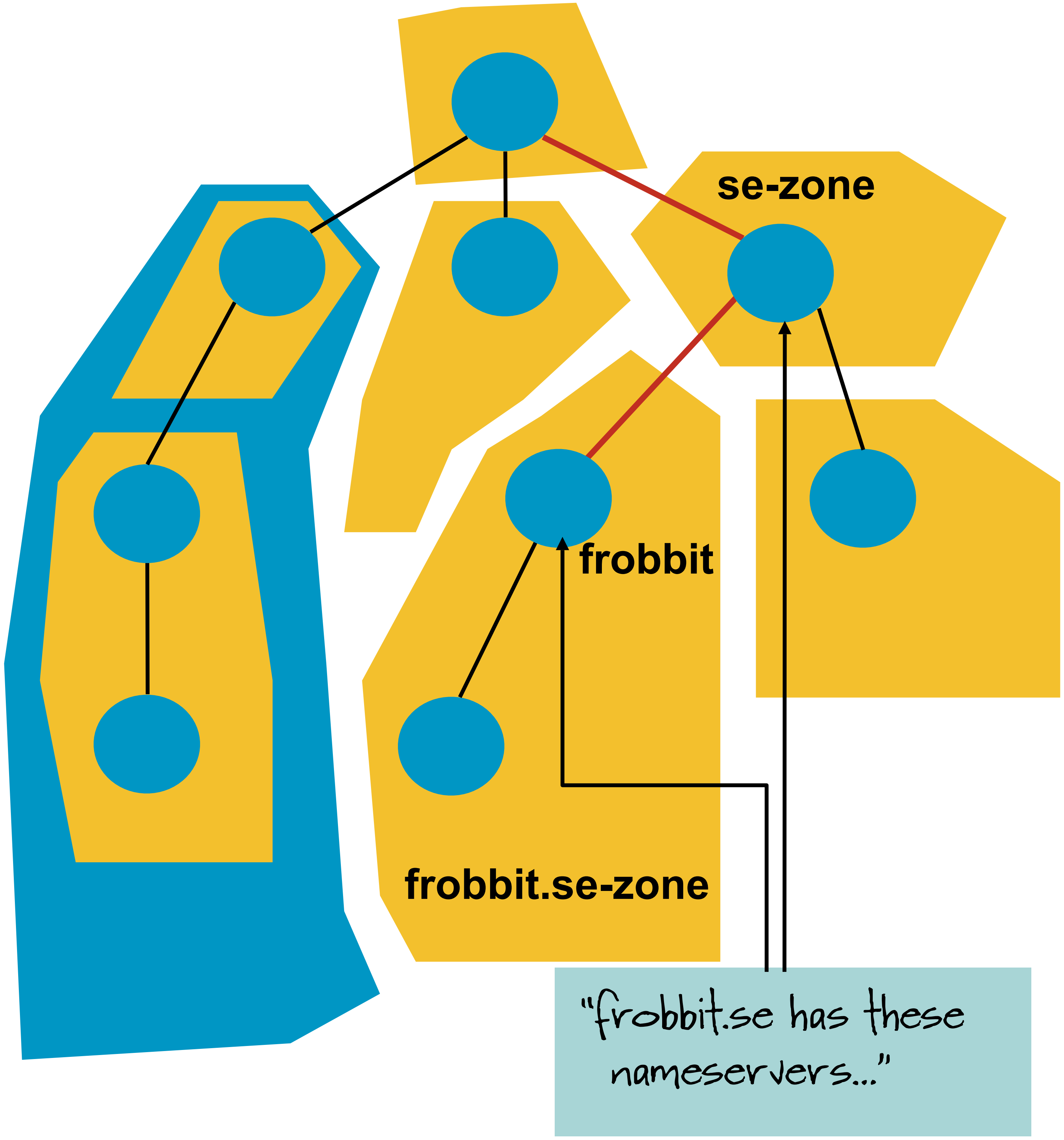
Resolvers and Queries

- We have clients which issue queries
  to servers

  Those are called "resolvers"

- Goal with DNS is to make sure resolvers find right server to send the query to

  Information in "parent" zone
  on where nameservers are for
  "child" zone



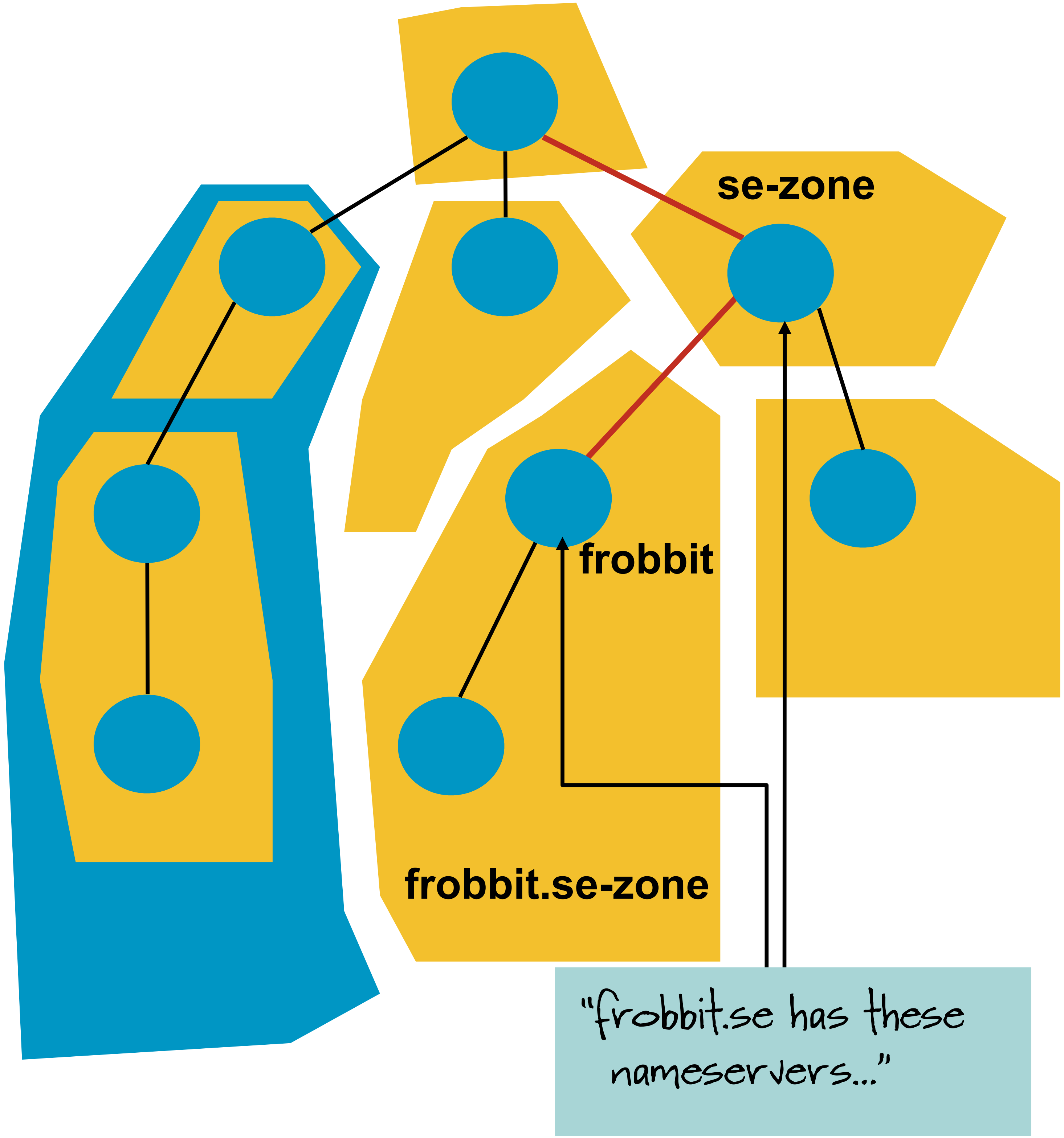
"frobbit.se has these
nameservers..."

Resolvers and Queries

- If the parent and child have different view on nameservers, there is something wrong

The information in parent zone has priority (child is authoritative)

Resolvers only find nameservers for child zone by sending query to parent



"frobbit.se has these nameservers..."

Forwarding- and authoritiative servers

- What is important?

  Your own hosts must be able to issue DNS queries

  Forwarding servers

  External hosts must be able to issue DNS queries about zones you administer

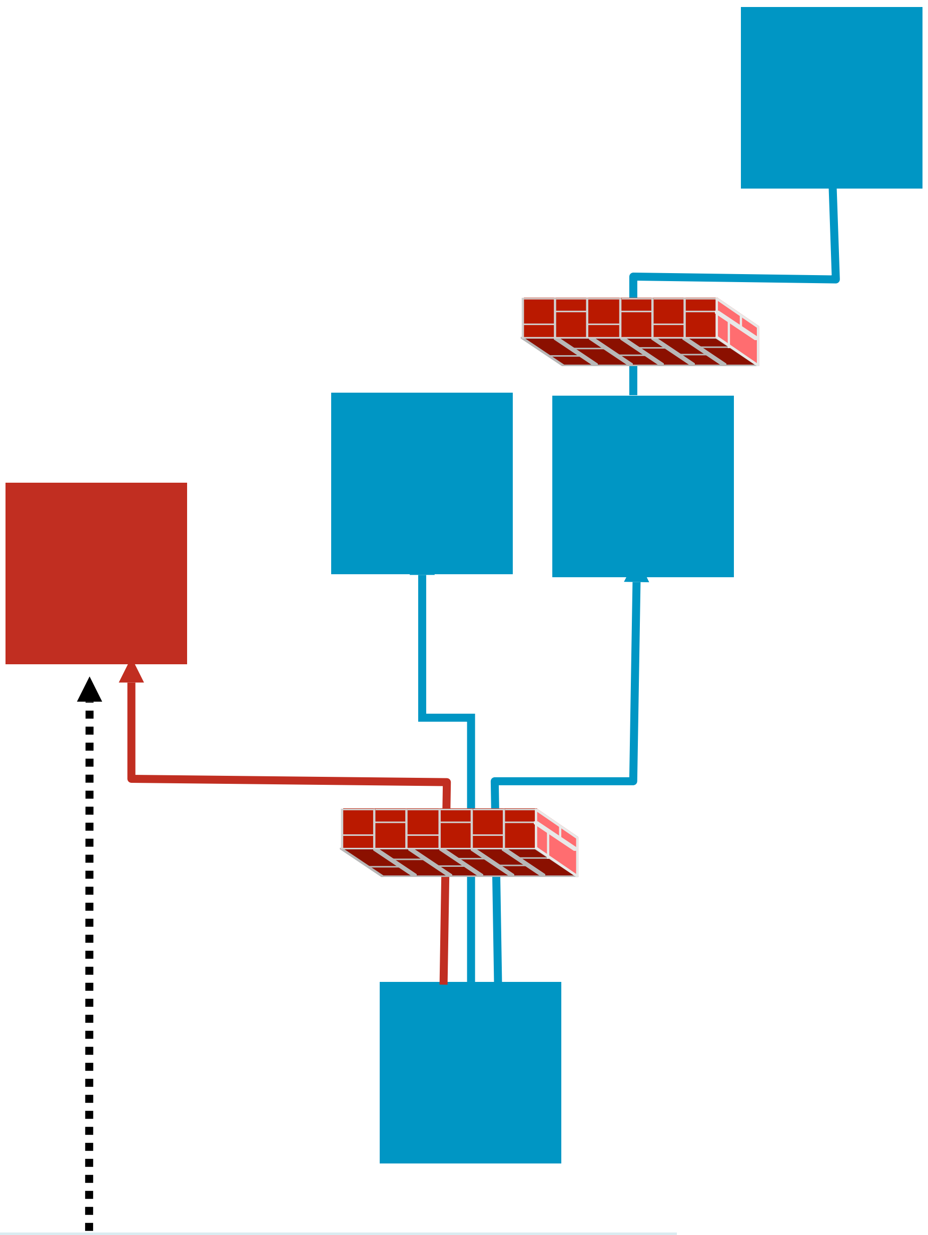
  Authoritative servers

- Two different problems, which should not be mixed up

Master, slave, etc.

- An authoritative server is a server that holds a zone directive for the zone (this implies it is either a master or a slave)
- A master server (or *primary*) is an authoritative server that allows outgoing zone transfers
- A primary master is the master server that holds the zone content
- A slave server (or *secondary*) is an authoritative server that copies zone content from a master server
- A stealth server is an authoritative server that is not referred to from parent zone (no NS records refer to a stealth server)
- A forwarding server accepts queries with recursion desired flag turned on (it will return answers with recursion available flag turned on)

Where are authoritative servers located?



Slave server(s) on
some other Network

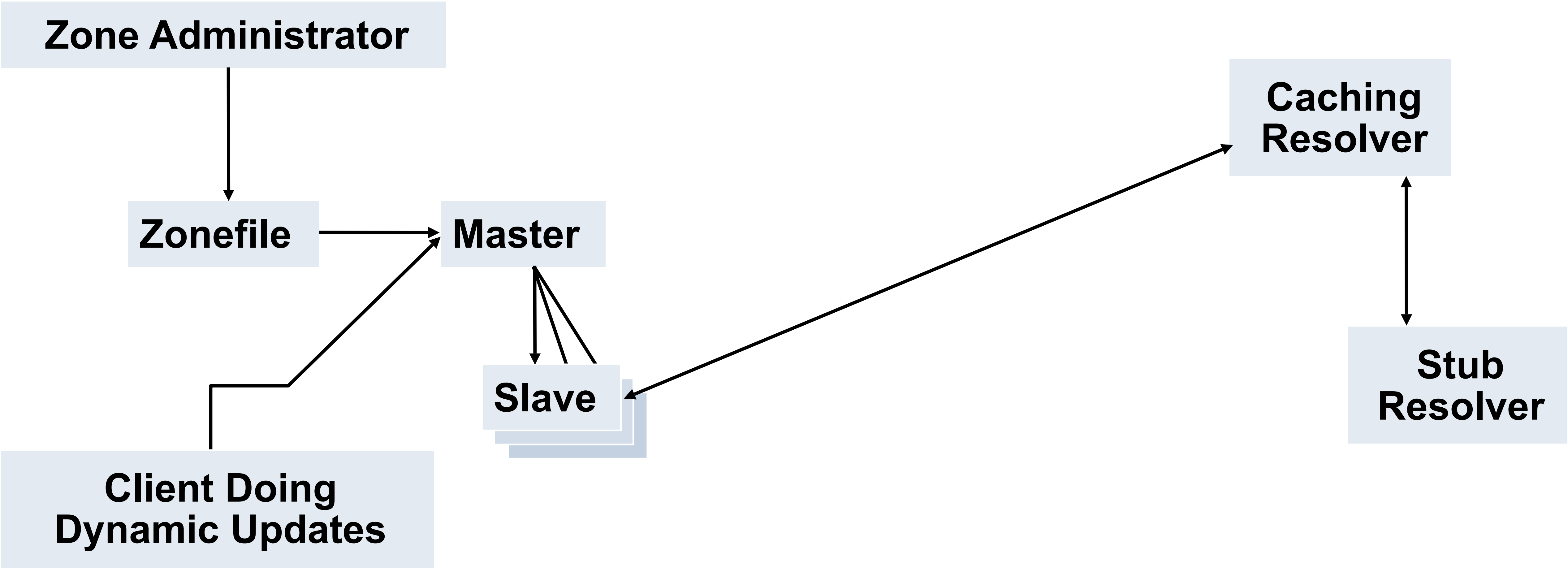
Slave servers in your DMZ

Forwarding server in DMZ,
not accessible from Internet

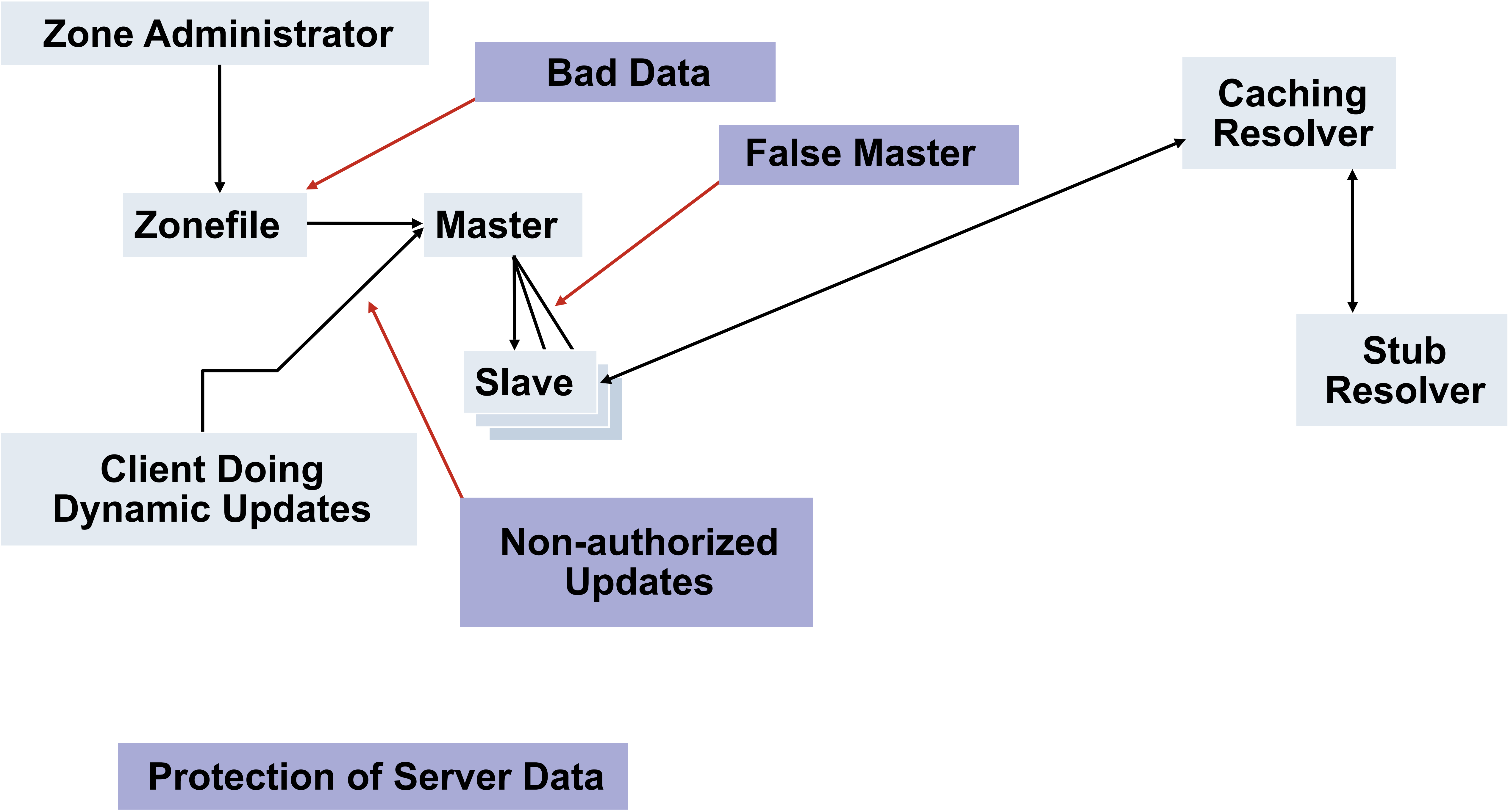
Hidden Master, not
accessible from Internet

Preloaded Forwarding server
(Stub Resolver)

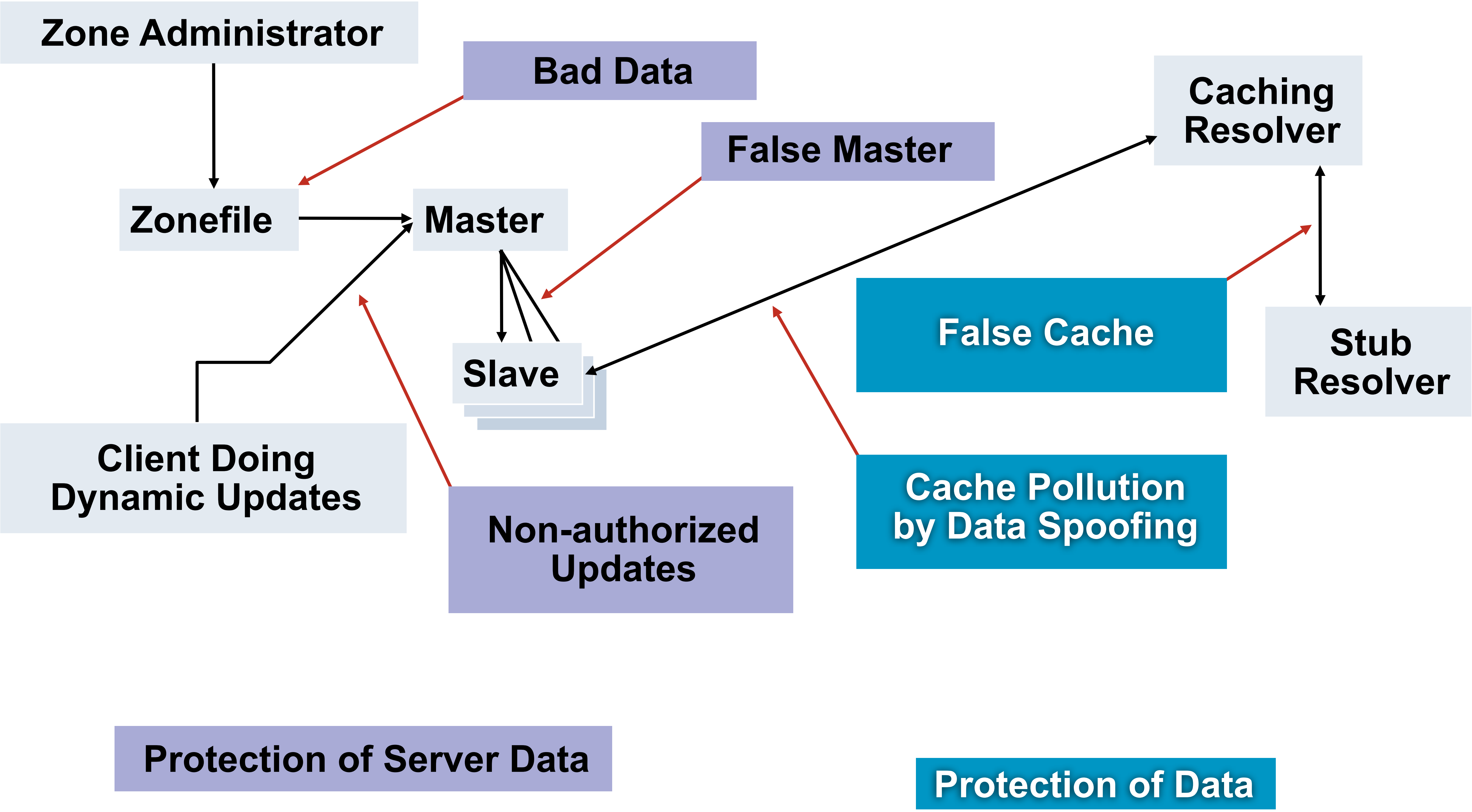
Security Issues with DNS



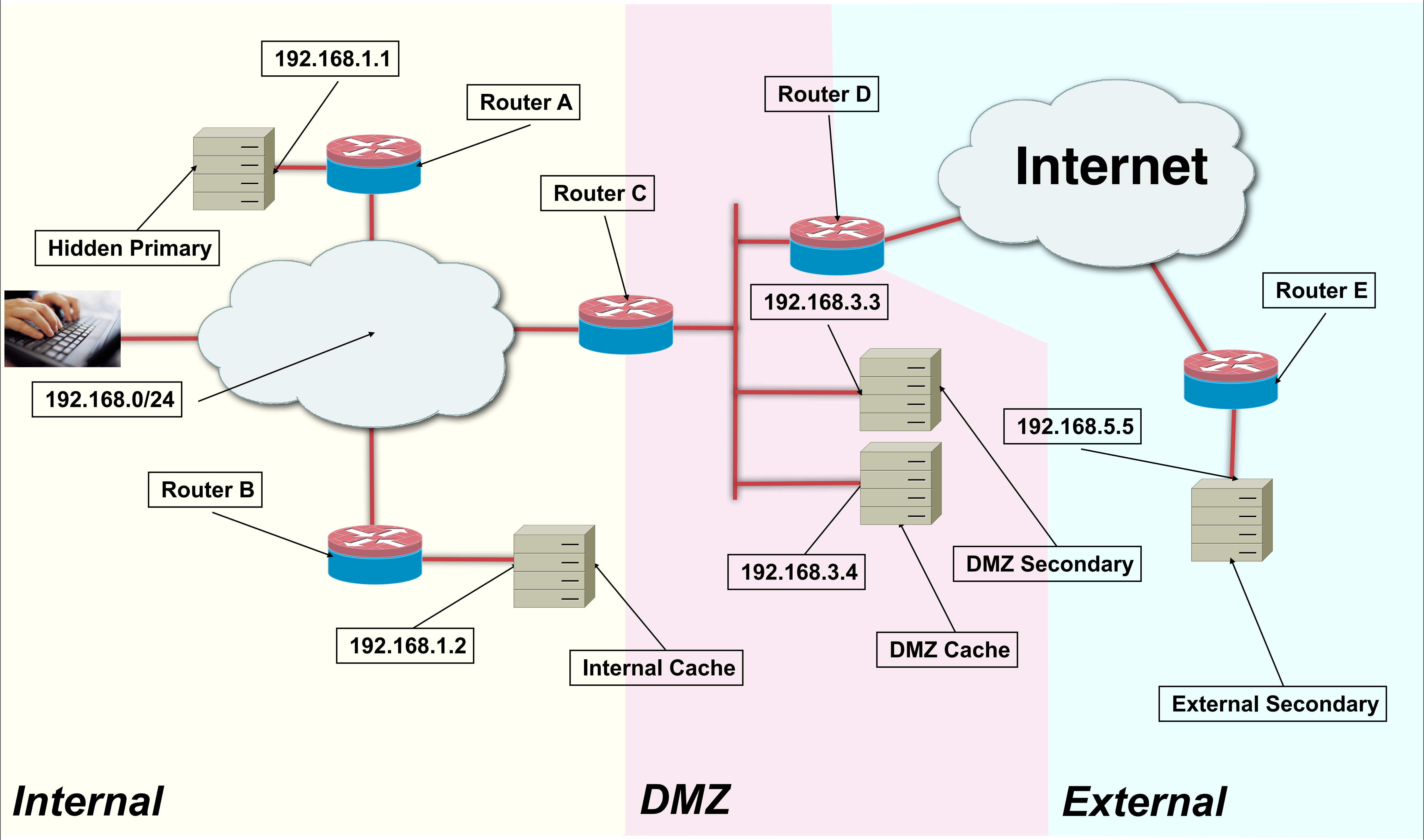
Security Issues with DNS



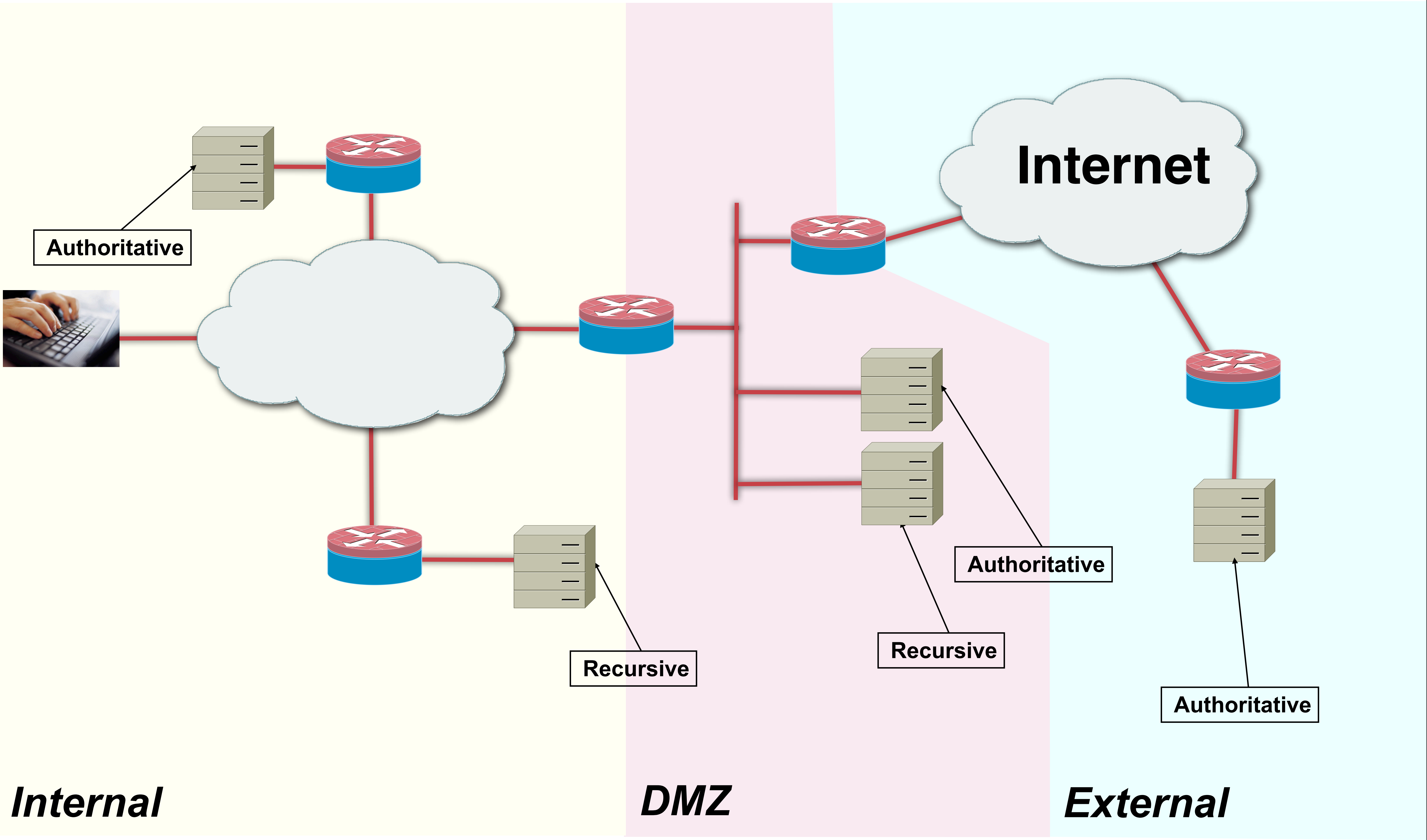
Security Issues with DNS



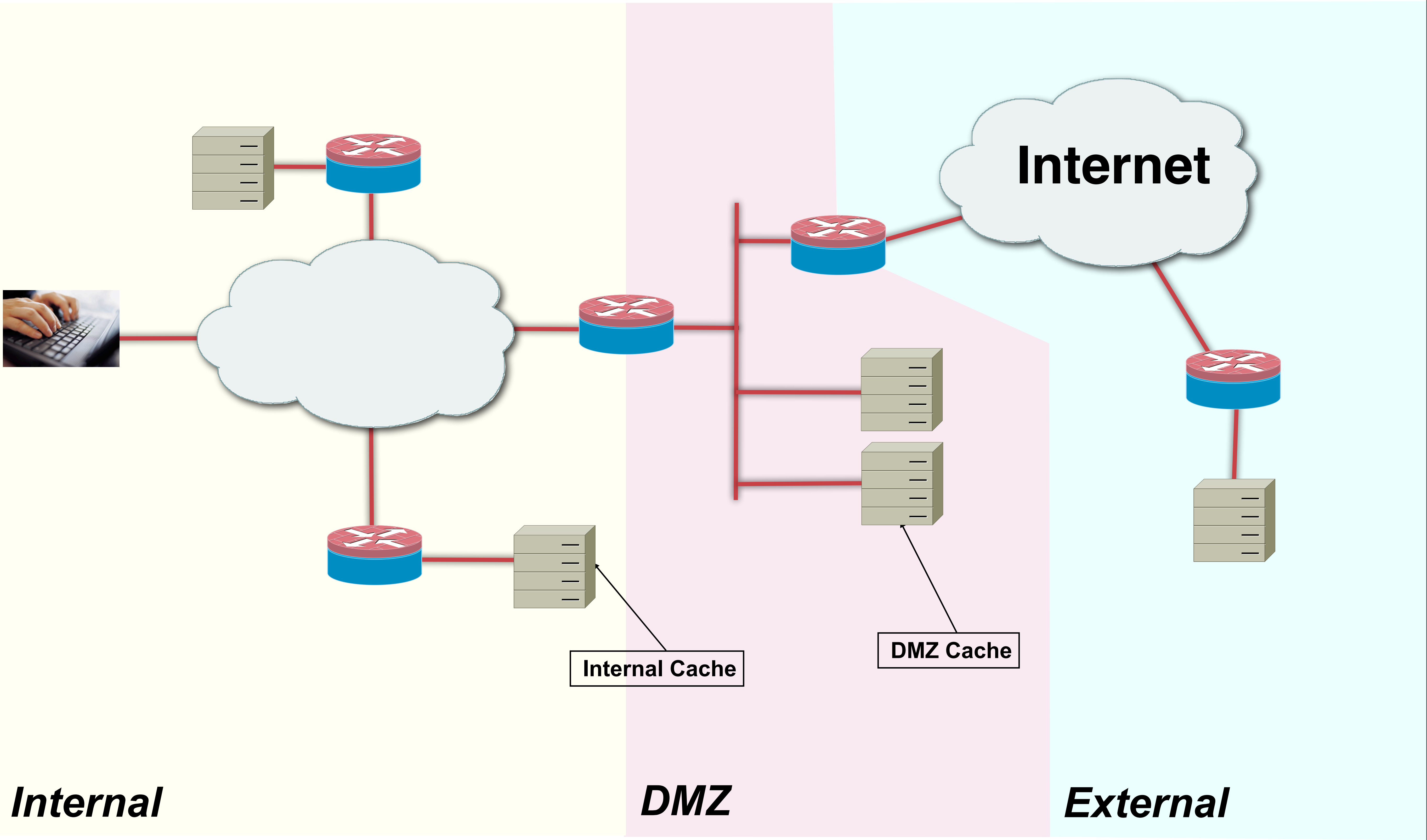
Detailed network layout



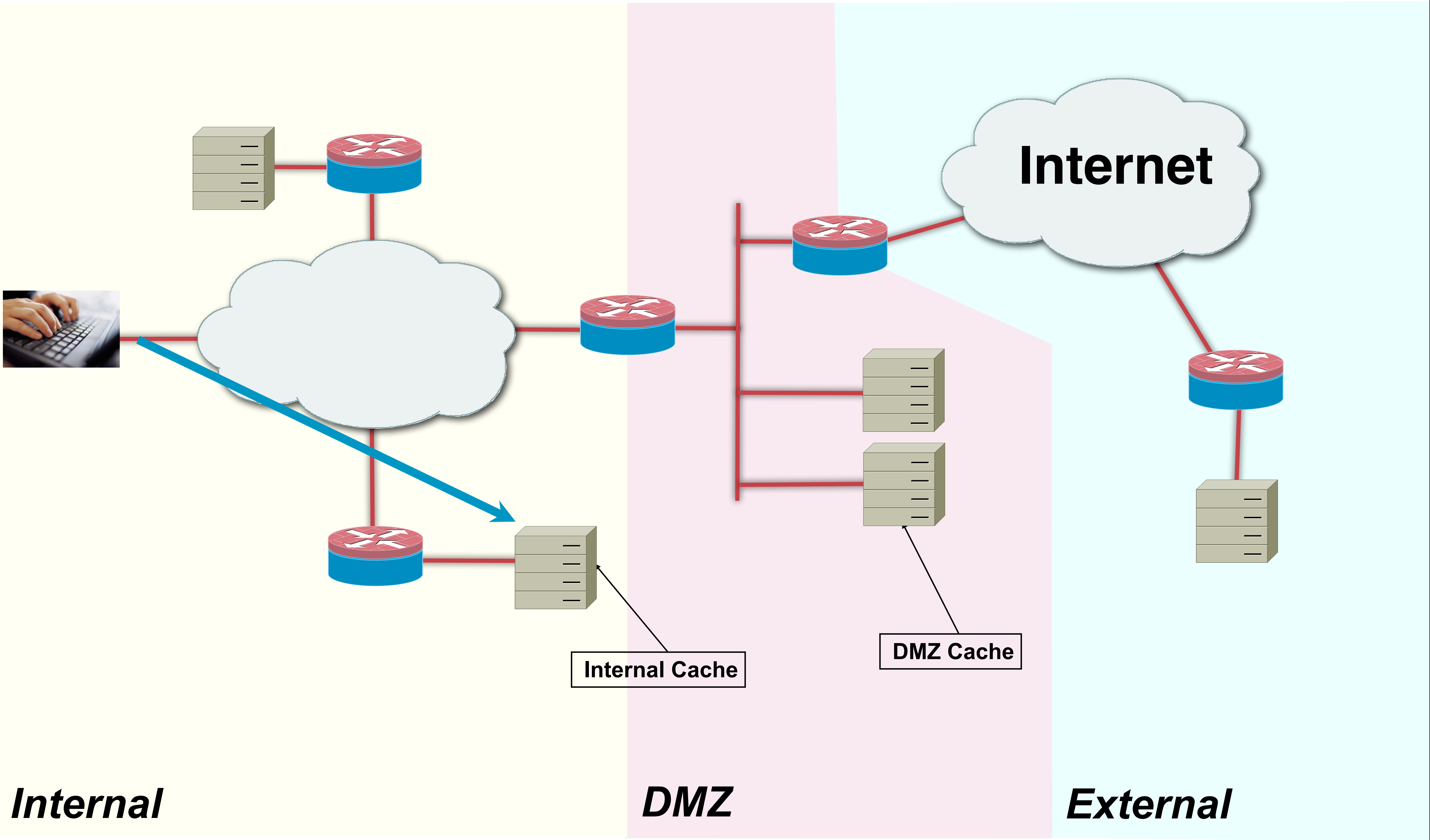
Different functions



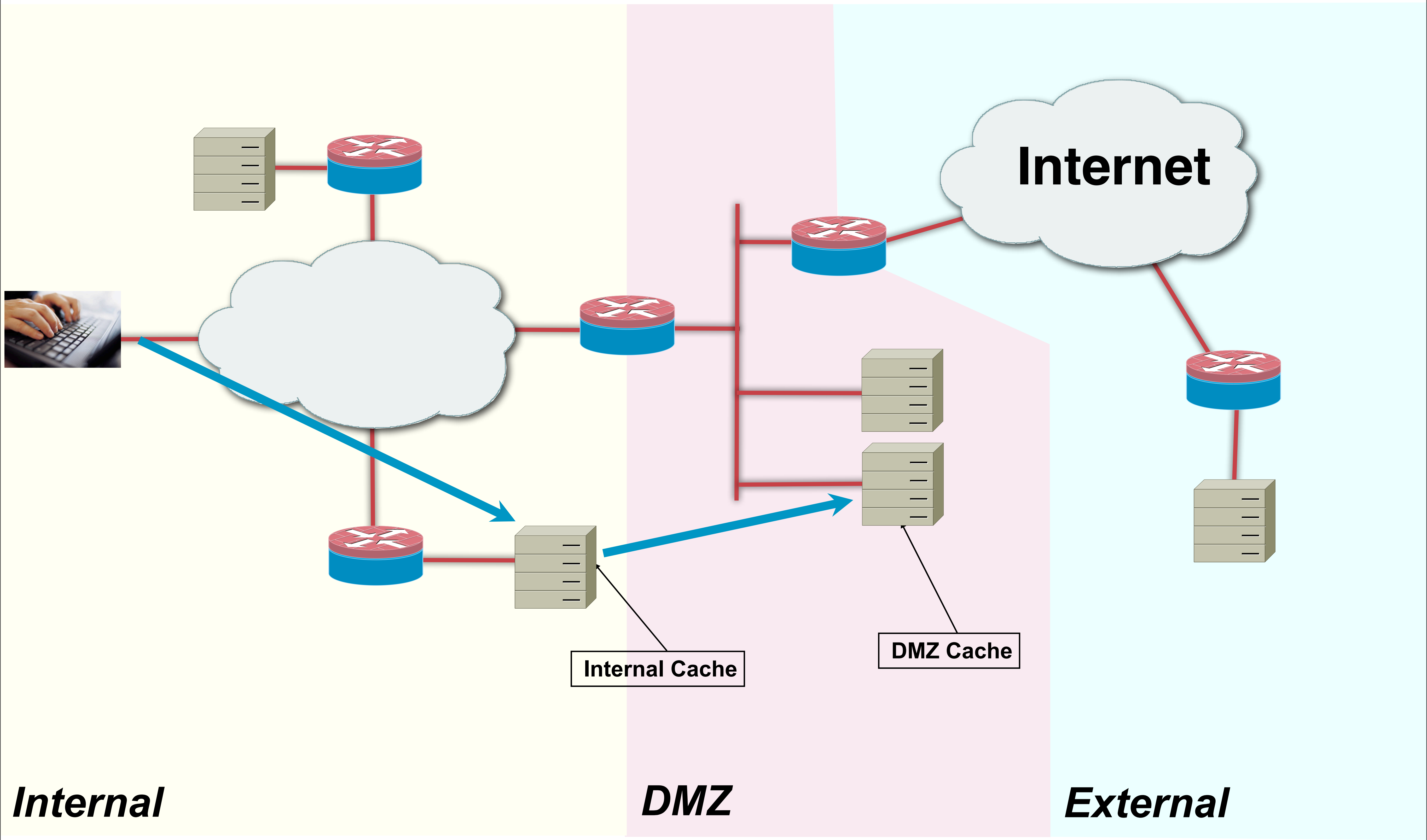
Queries from the inside



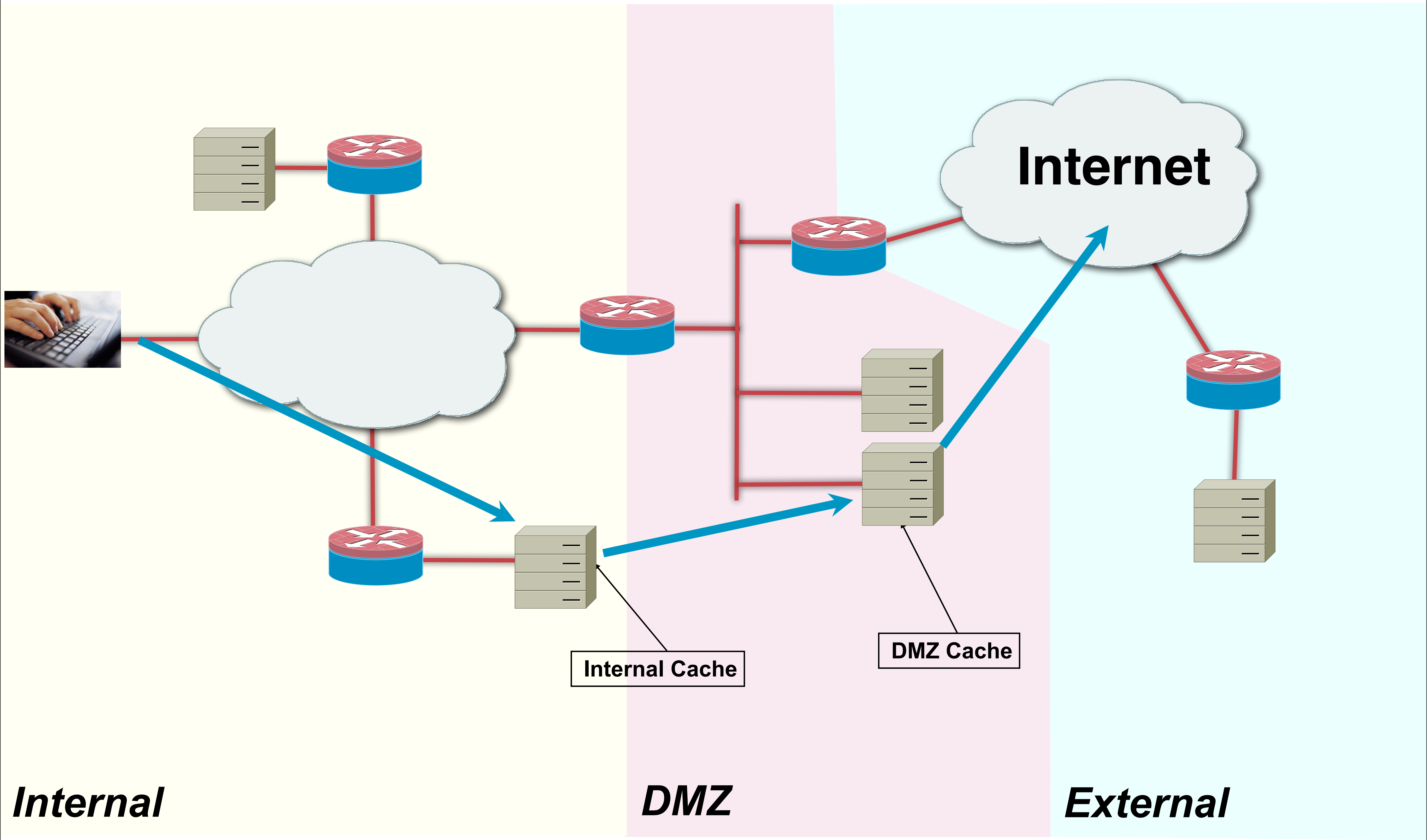
Queries from the inside



Queries from the inside



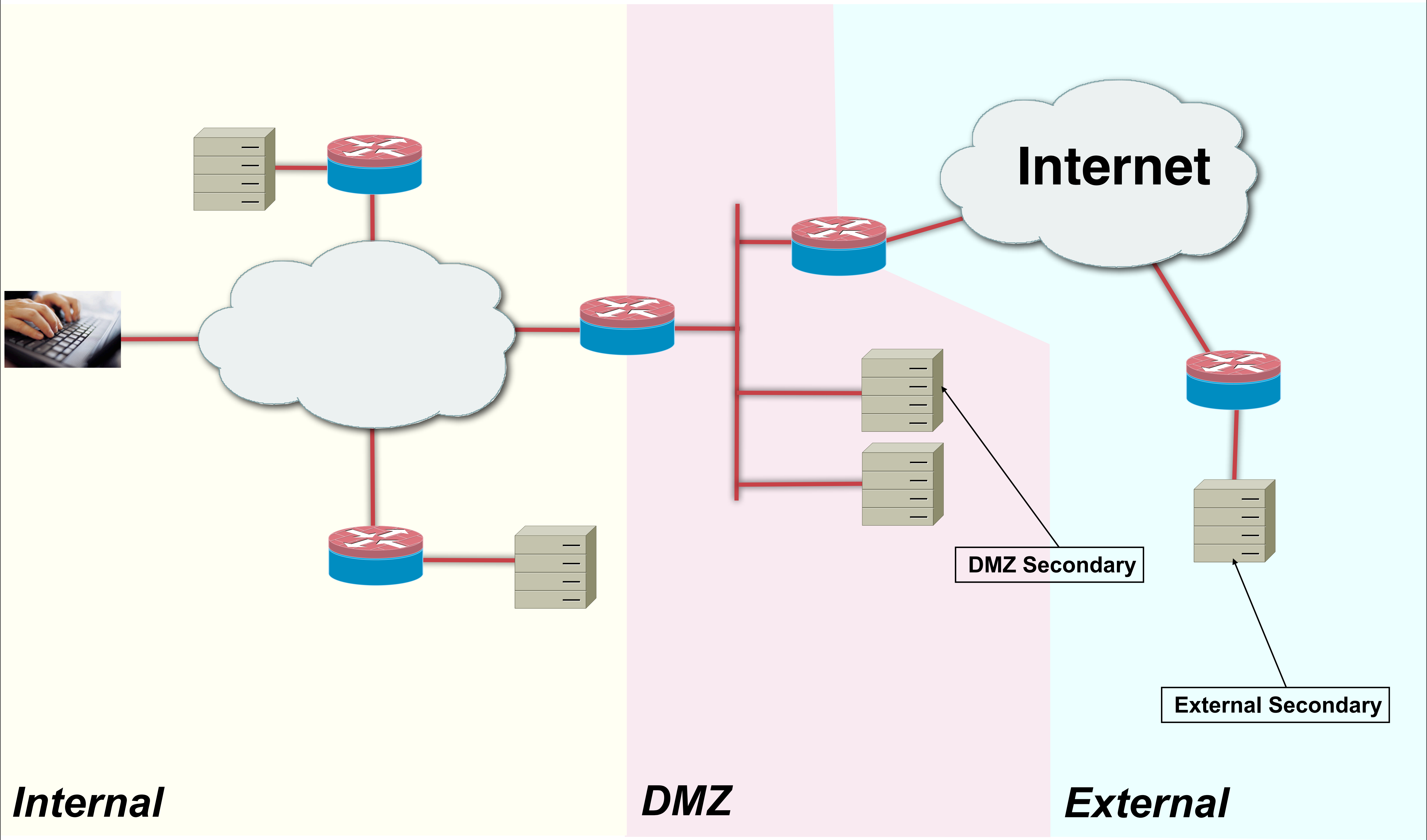
Queries from the inside



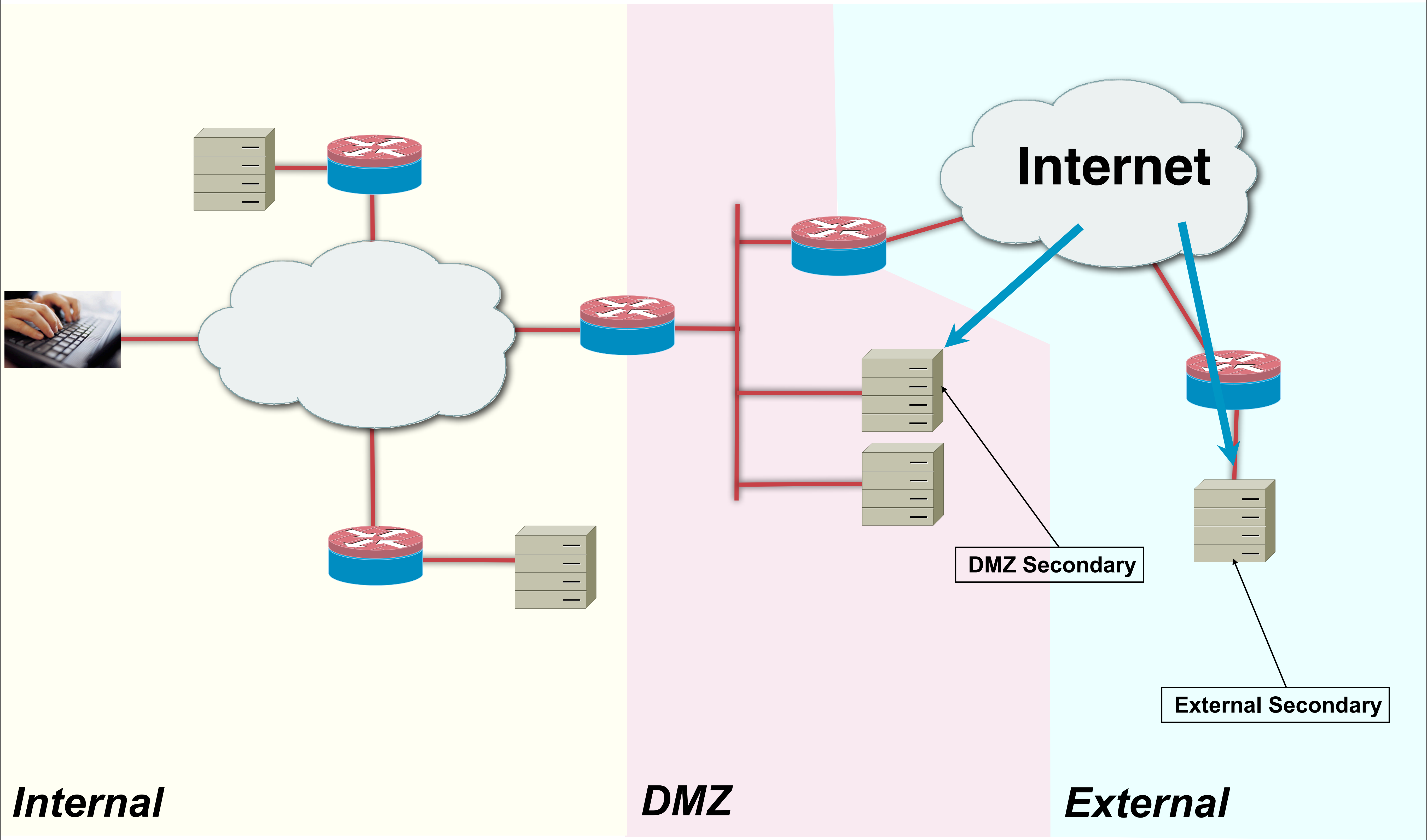
Public

måndag 3 november 2008

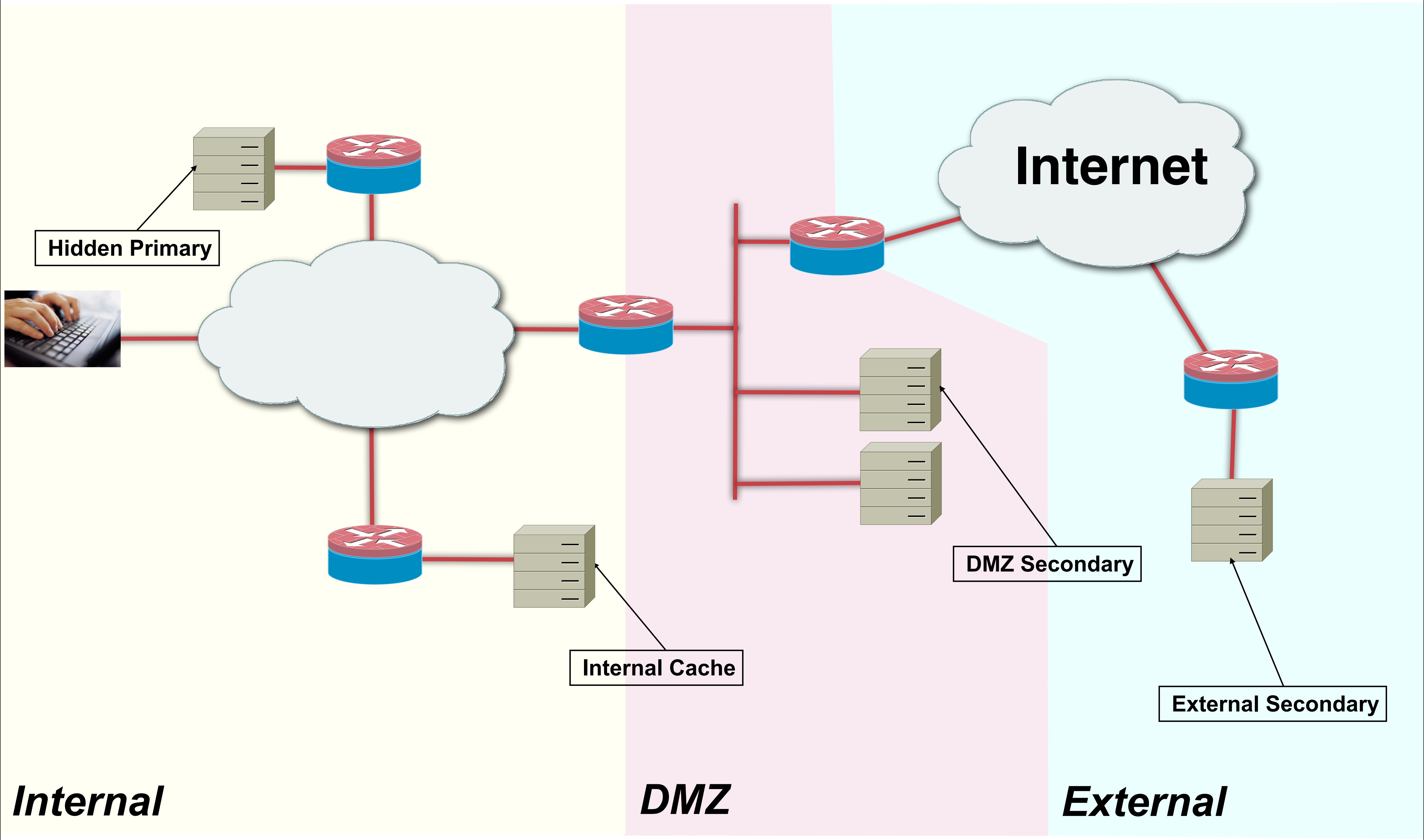
Queries from the outside



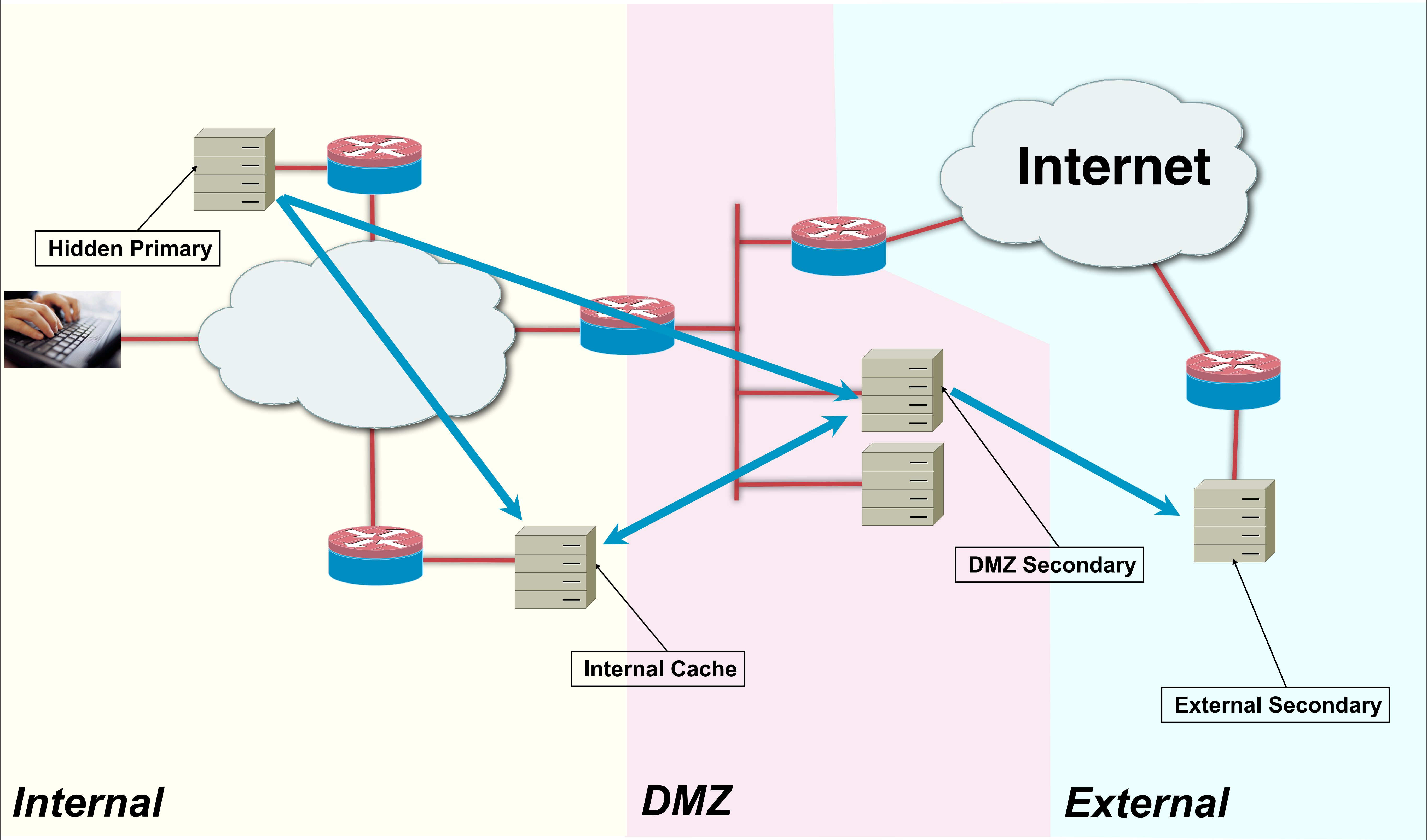
Queries from the outside



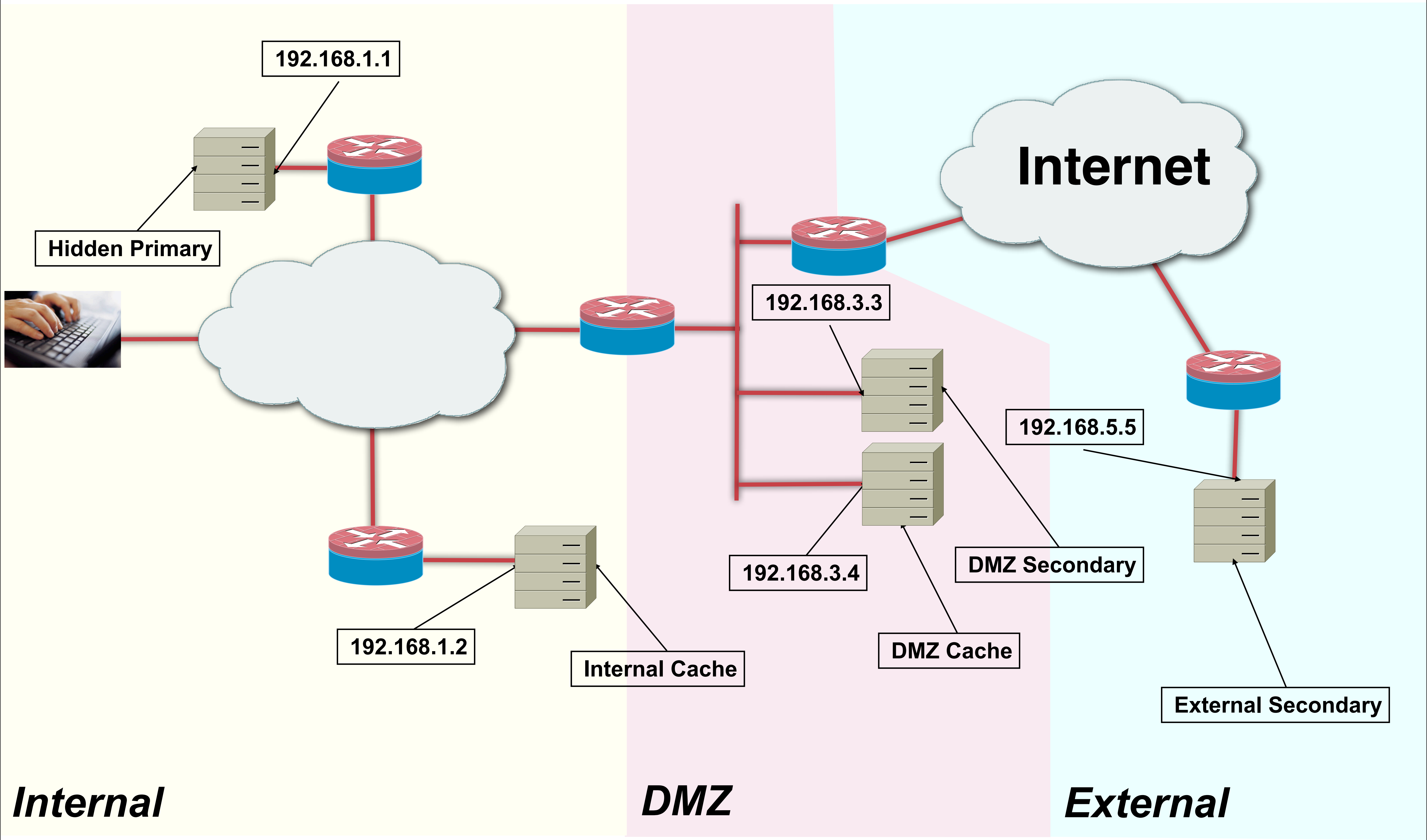
Zone transfer



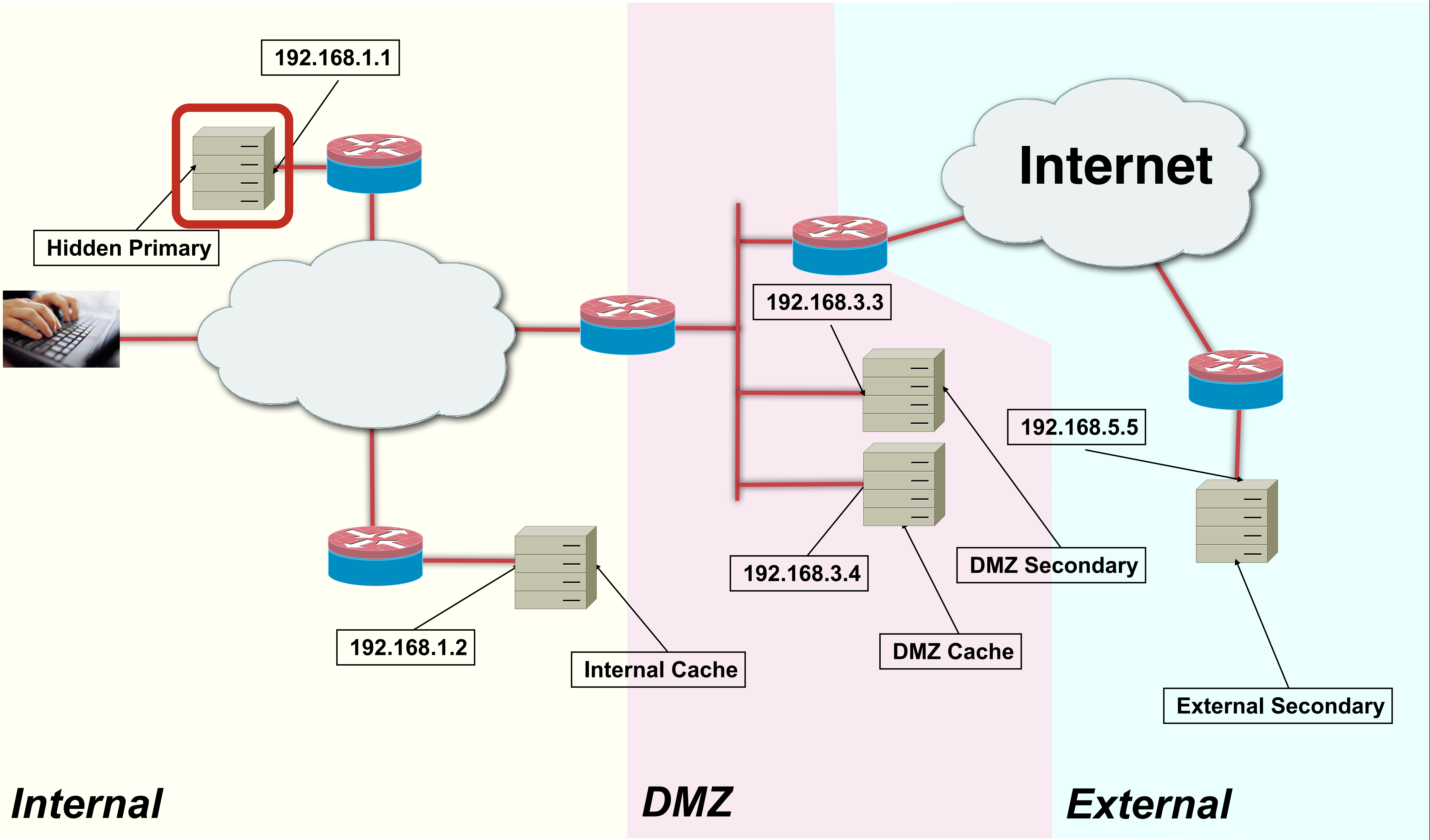
Zone transfer



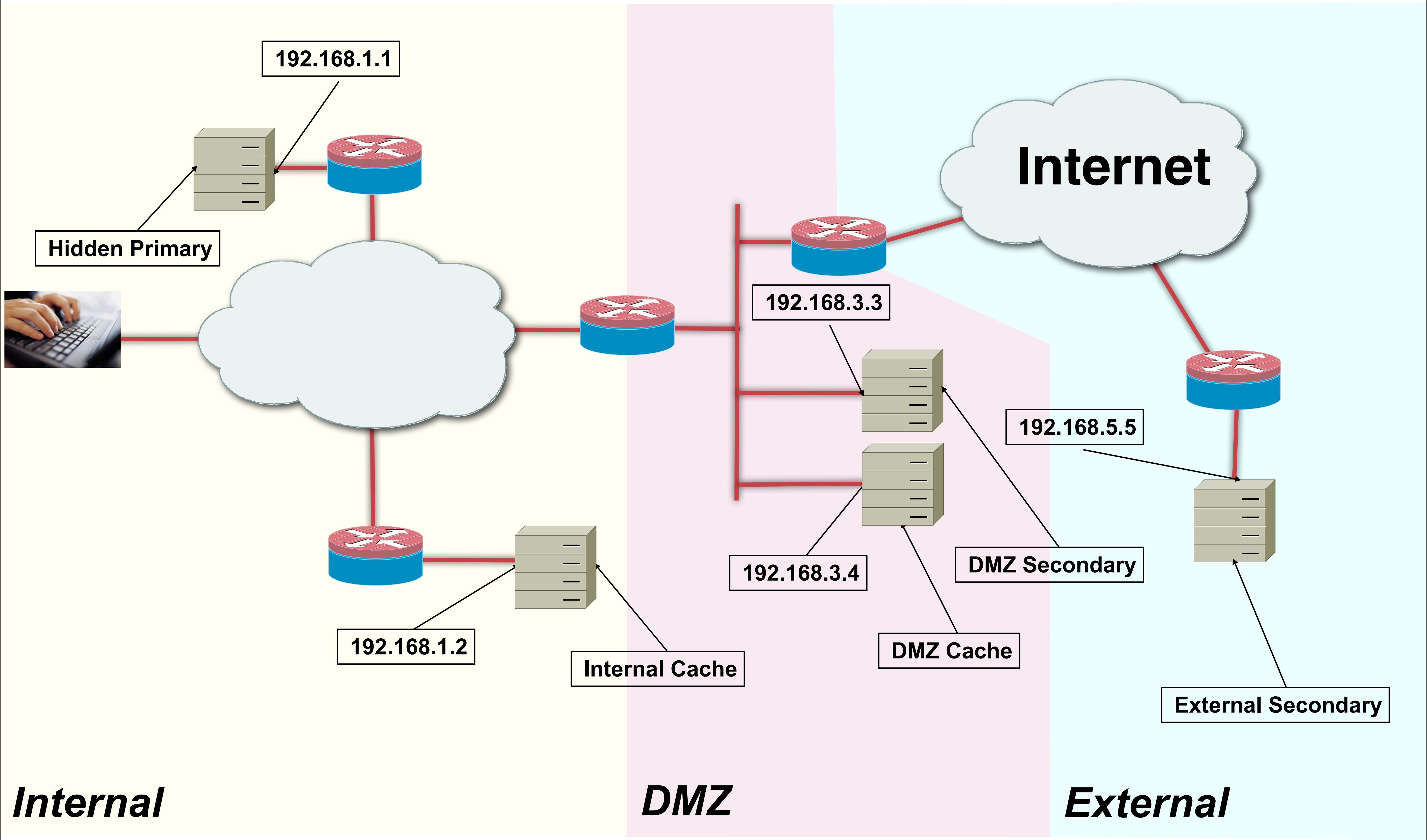
Hidden primary, Authoritative, DNSSEC



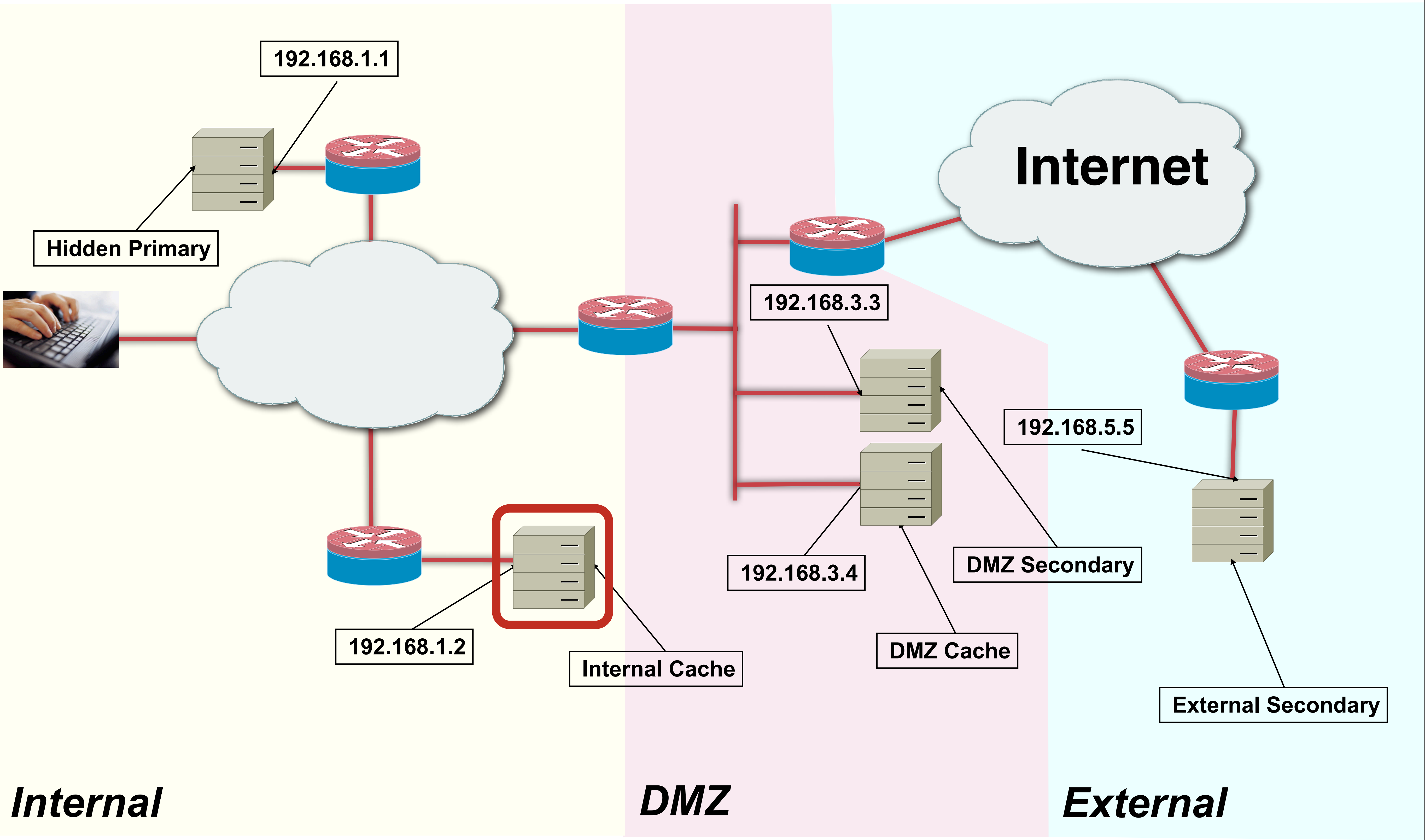
Hidden primary, Authoritative, DNSSEC



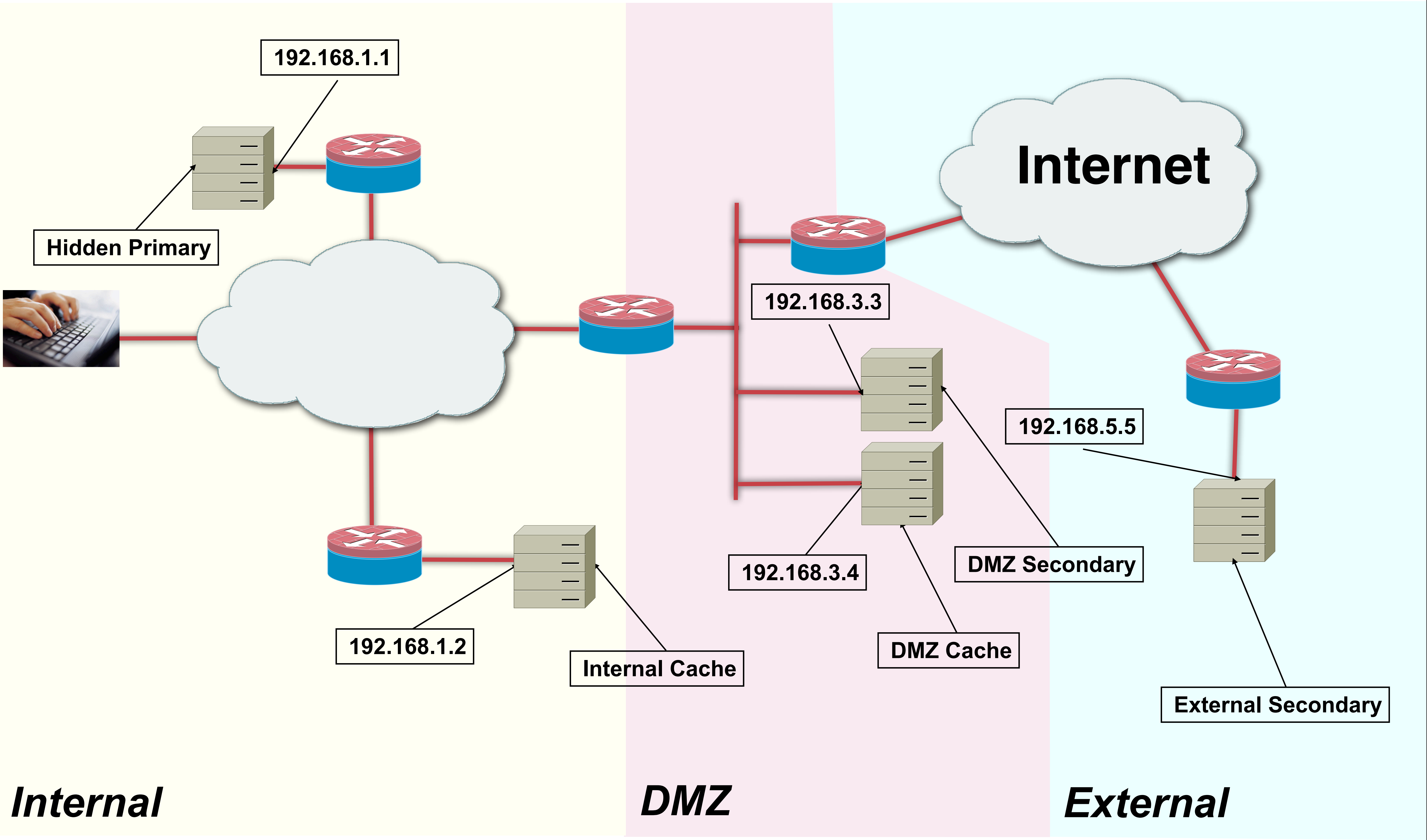
Internal Cache, Recursive



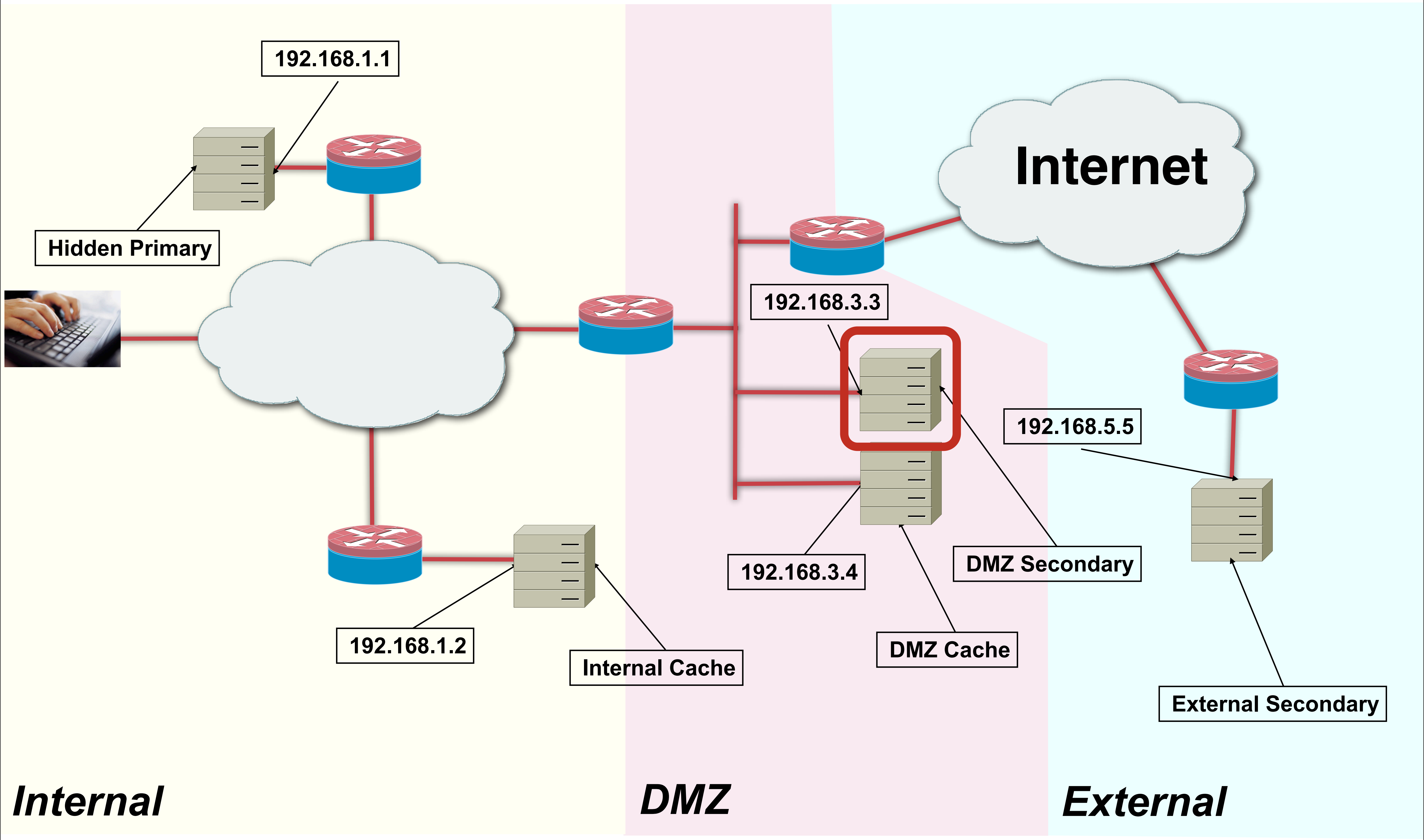
Internal Cache, Recursive



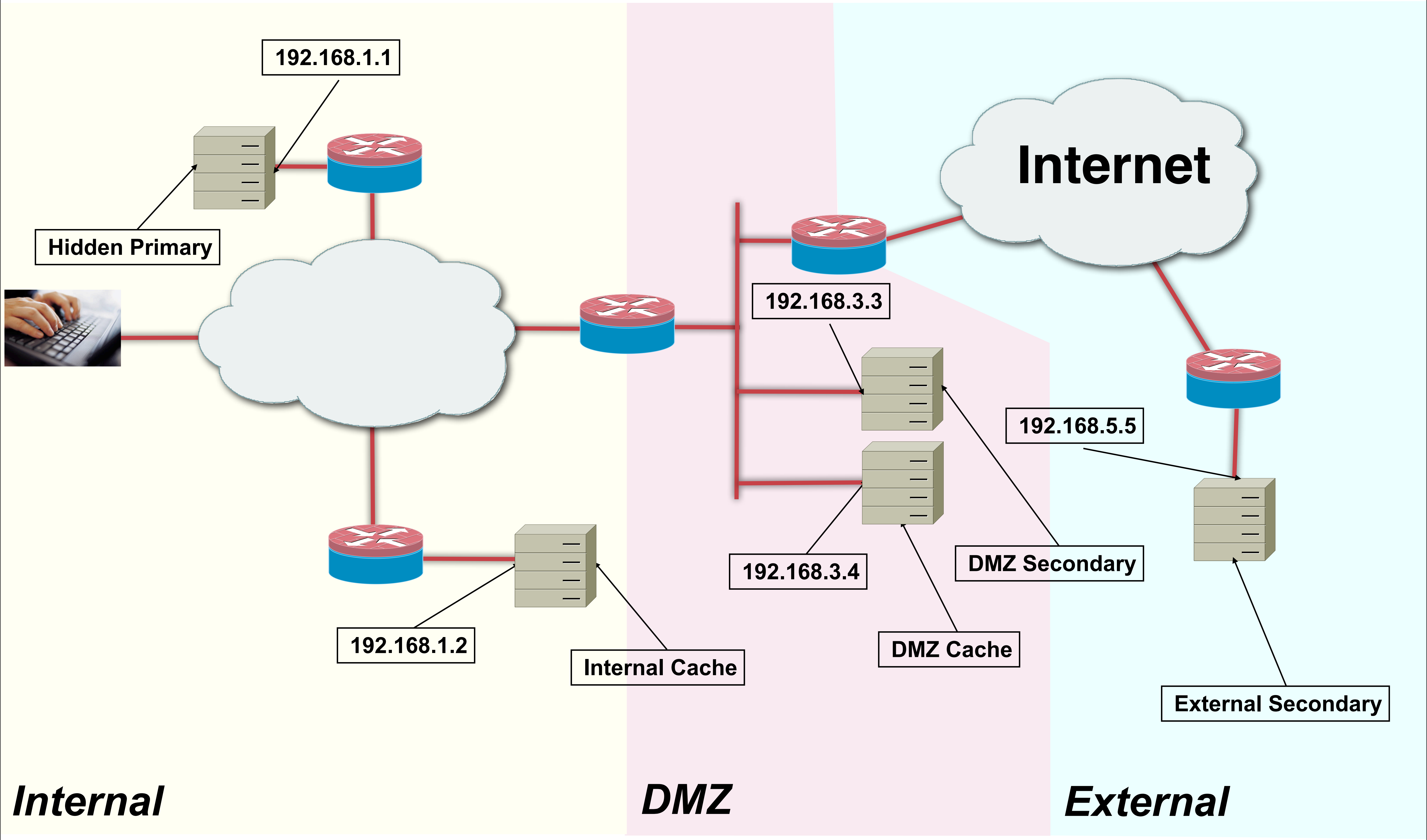
DMZ Secondary, Authoritative



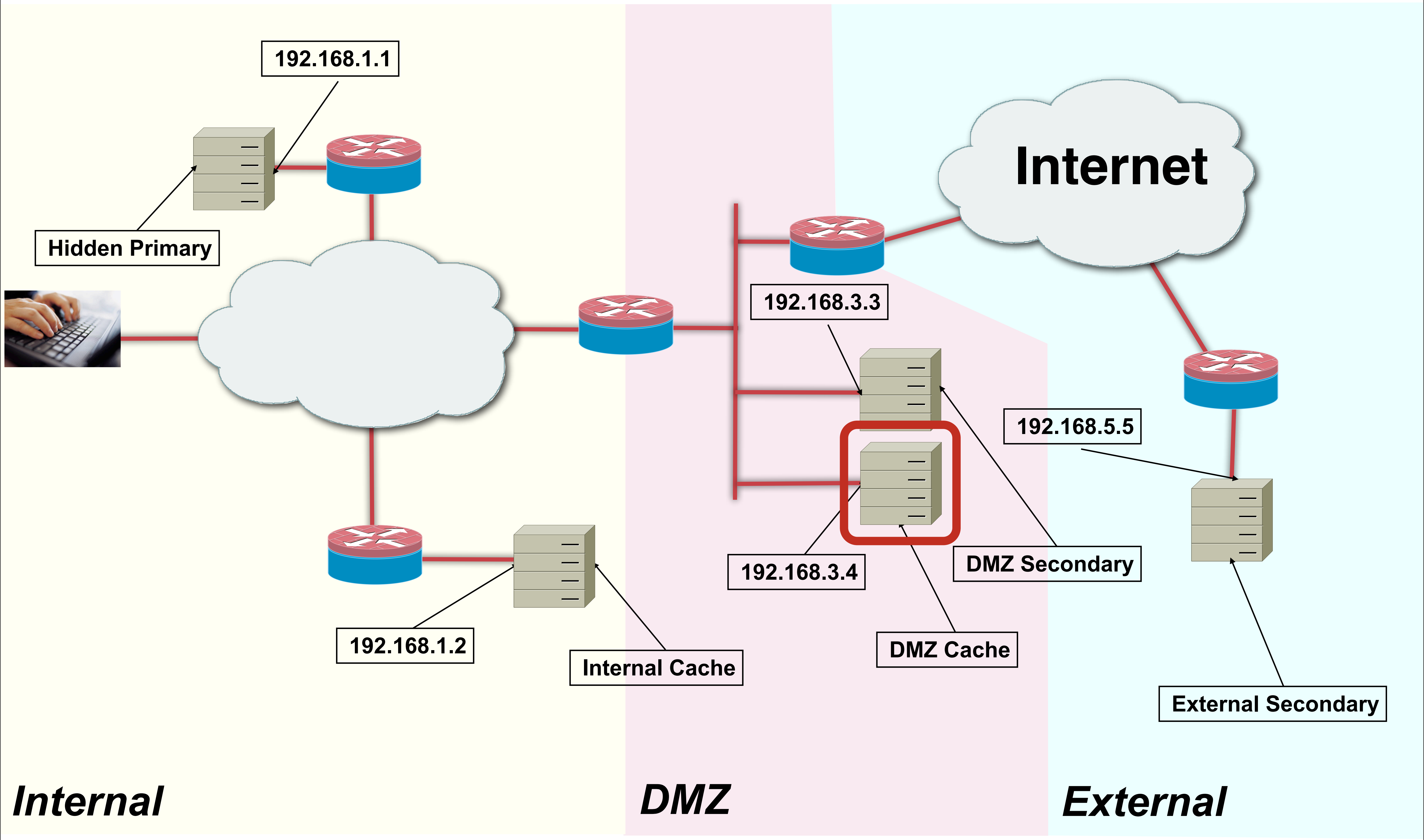
DMZ Secondary, Authoritative



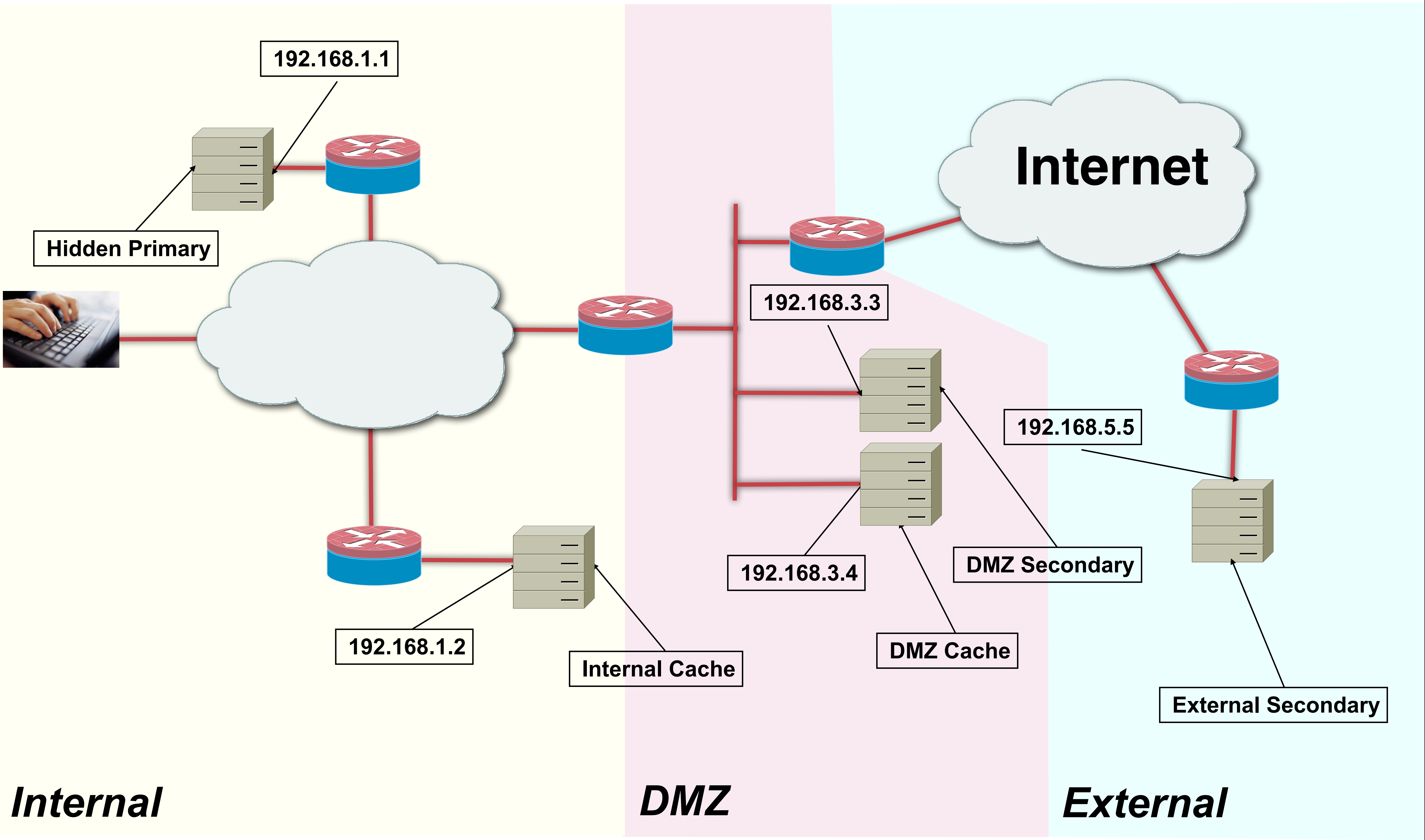
DMZ Cache, Recursive



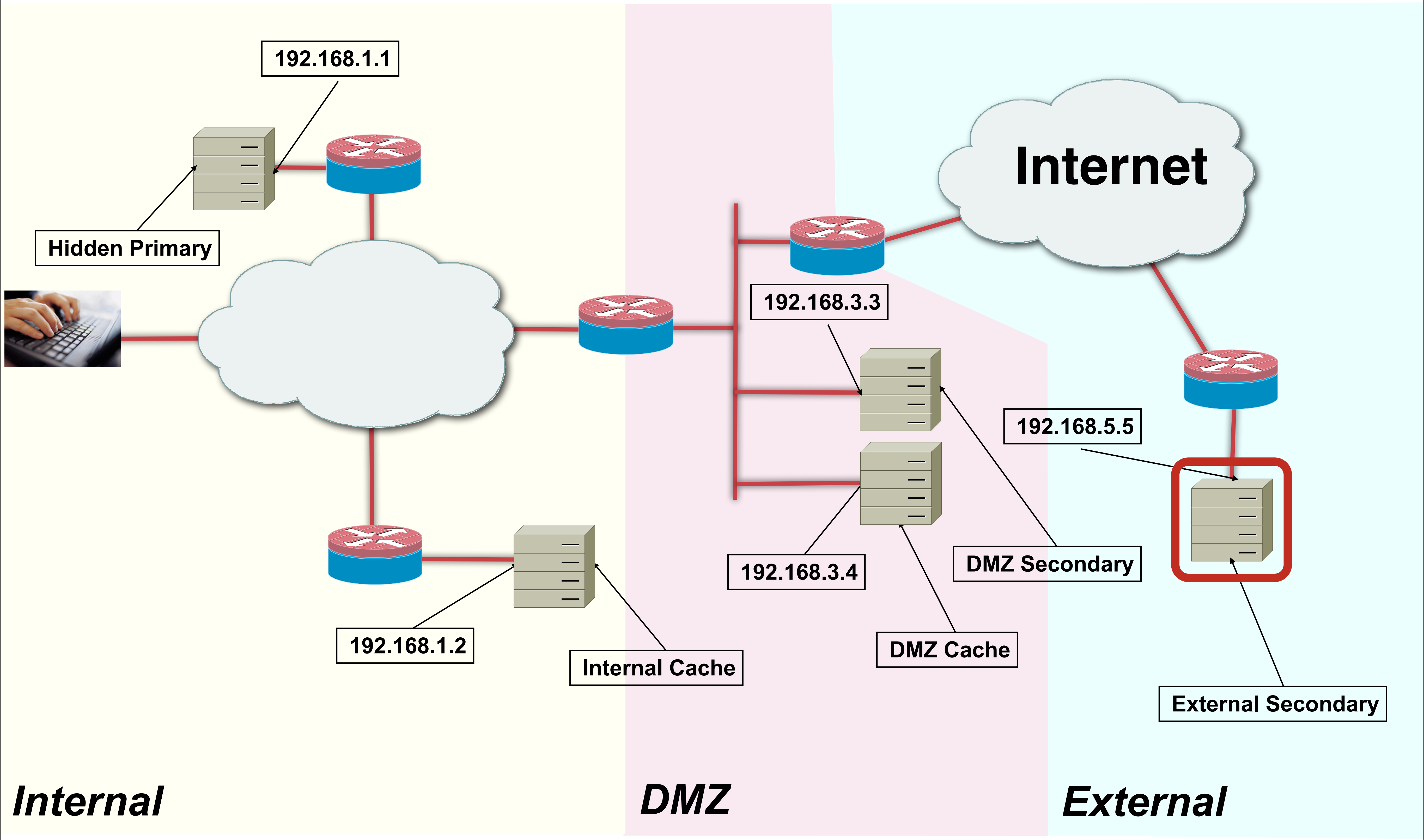
DMZ Cache, Recursive



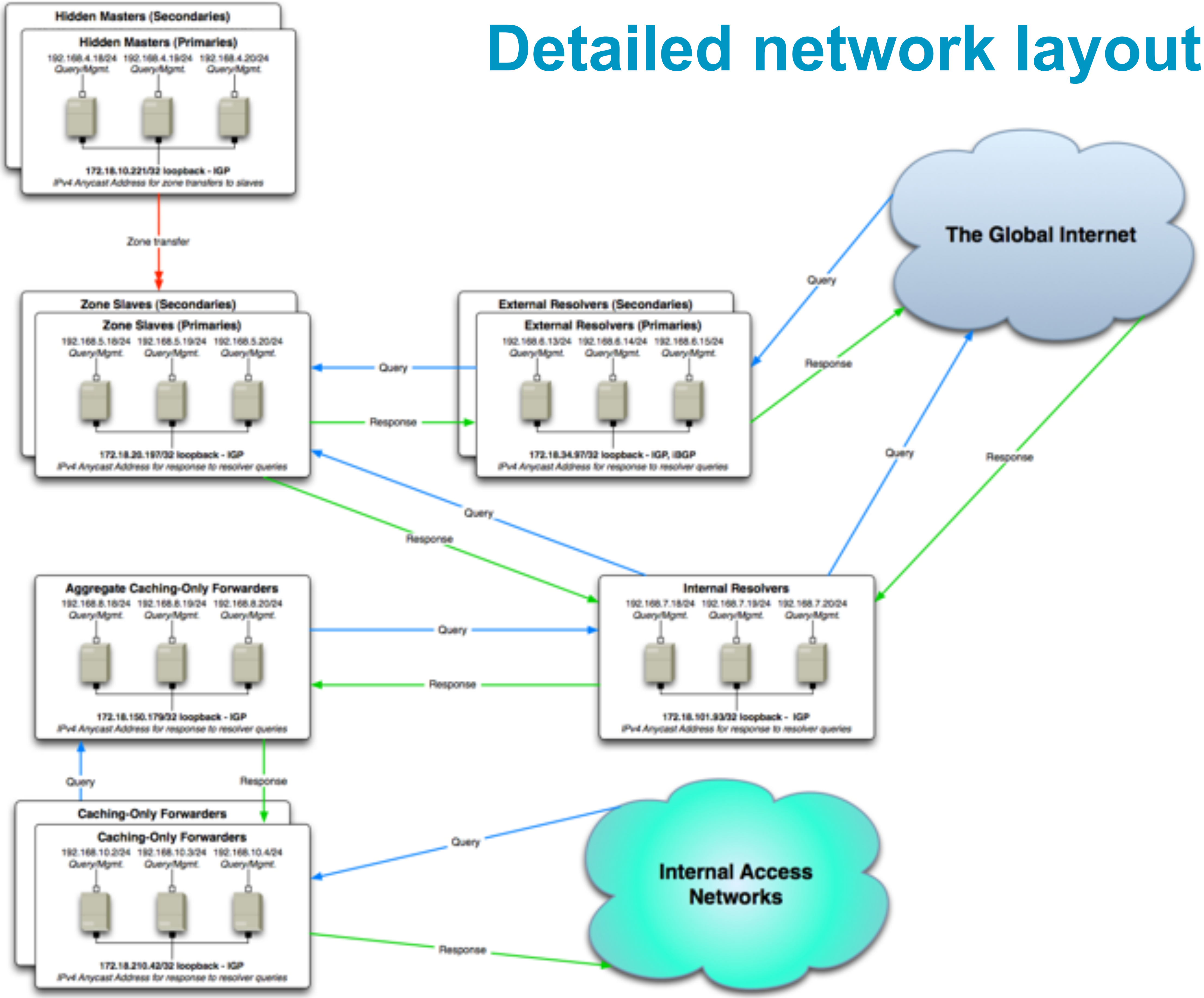
External Secondary, Authoritative



External Secondary, Authoritative



Detailed network layout


Hidden Masters (Secondaries)
Hidden Masters (Primaries)
192.168.4.18/24 Query/Mgmt.
192.168.4.19/24 Query/Mgmt.
192.168.4.20/24 Query/Mgmt.
172.18.10.221/32 loopback - IGP
IPv4 Anycast Address for zone transfers to slaves
Zone transfer
The Global Internet
Zone Slaves (Secondaries)
Zone Slaves (Primaries)
192.168.5.18/24 Query/Mgmt.
192.168.5.19/24 Query/Mgmt.
192.168.5.20/24 Query/Mgmt.
172.18.20.197/32 loopback - IGP
IPv4 Anycast Address for response to resolver queries
Query
Response
External Resolvers (Secondaries)
External Resolvers (Primaries)
192.168.6.13/24 Query/Mgmt.
192.168.6.14/24 Query/Mgmt.
192.168.6.15/24 Query/Mgmt.
172.18.34.97/32 loopback - IGP, IBGP
IPv4 Anycast Address for response to resolver queries
Query
Response
Query
Response
Query
Response
Aggregate Caching-Only Forwarders
192.168.8.18/24 Query/Mgmt.
192.168.8.19/24 Query/Mgmt.
192.168.8.20/24 Query/Mgmt.
172.18.150.179/32 loopback - IGP
IPv4 Anycast Address for response to resolver queries
Query
Response
Internal Resolvers
192.168.7.18/24 Query/Mgmt.
192.168.7.19/24 Query/Mgmt.
192.168.7.20/24 Query/Mgmt.
172.18.101.93/32 loopback - IGP
IPv4 Anycast Address for response to resolver queries
Query
Response
Caching-Only Forwarders
Caching-Only Forwarders
192.168.10.2/24 Query/Mgmt.
192.168.10.3/24 Query/Mgmt.
192.168.10.4/24 Query/Mgmt.
172.18.210.42/32 loopback - IGP
IPv4 Anycast Address for response to resolver queries
Query
Response
Internal Access Networks

Conclusion

- A good DNS setup includes the following:

  Master server where zone data is stored that can not be reached from the Internet

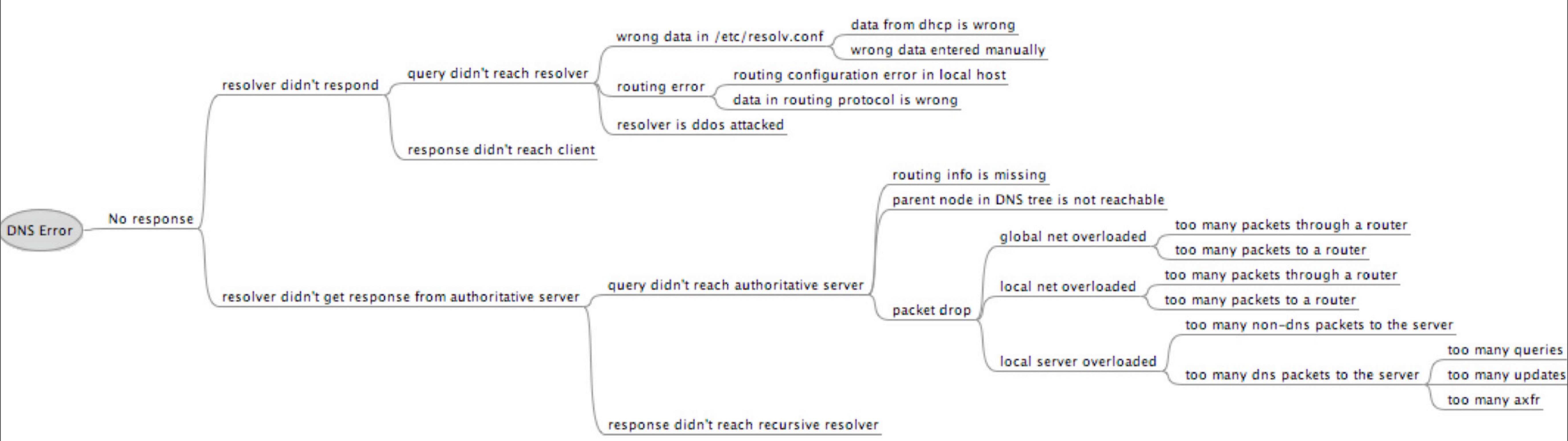
  Slave servers that receive queries from the Internet

  Separate forwarding server that has local zones preloaded, so lookup of local zones never fail

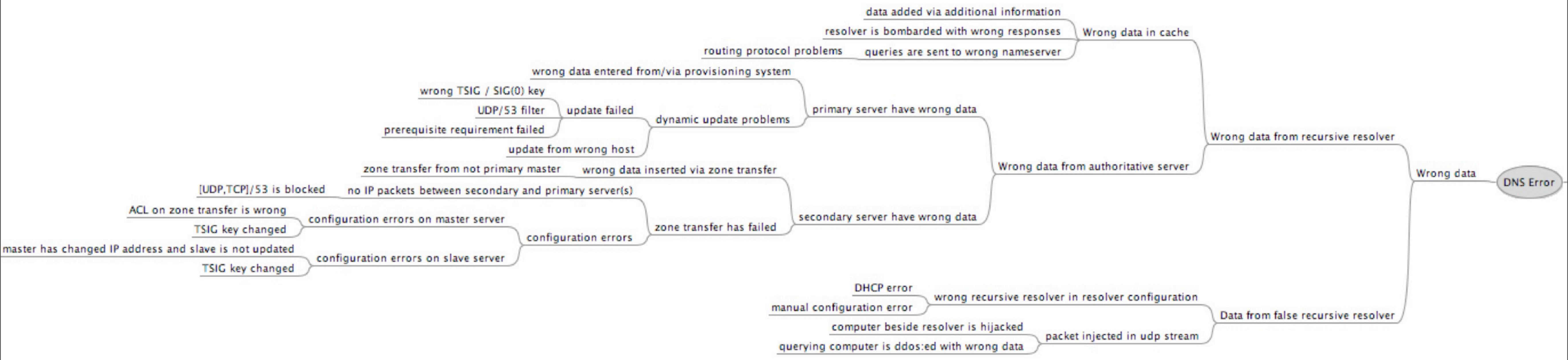
  Use of Notify so all authoritative servers have up to date information about the zones

  Secure the servers themselves so they can not be used for services they are not designed for

Questions?



- DNS Error
  - No response
    - resolver didn't respond
      - query didn't reach resolver
        - wrong data in /etc/resolv.conf
          - data from dhcp is wrong
          - wrong data entered manually
        - routing error
          - routing configuration error in local host
          - data in routing protocol is wrong
        - resolver is ddos attacked
      - response didn't reach client
    - resolver didn't get response from authoritative server
      - query didn't reach authoritative server
        - routing info is missing
        - parent node in DNS tree is not reachable
        - packet drop
          - global net overloaded
            - too many packets through a router
            - too many packets to a router
          - local net overloaded
            - too many packets through a router
            - too many packets to a router
          - local server overloaded
            - too many non-dns packets to the server
            - too many dns packets to the server
              - too many queries
              - too many updates
              - too many axfr
      - response didn't reach recursive resolver



- DNS Error
  - Wrong data
    - Wrong data from recursive resolver
      - Wrong data in cache
        - data added via additional information
        - resolver is bombarded with wrong responses
        - queries are sent to wrong nameserver
          - routing protocol problems
      - Wrong data from authoritative server
        - primary server have wrong data
          - wrong data entered from/via provisioning system
          - dynamic update problems
            - update failed
              - wrong TSIG / SIG(0) key
              - UDP/53 filter
              - prerequisite requirement failed
            - update from wrong host
        - secondary server have wrong data
          - wrong data inserted via zone transfer
            - zone transfer from not primary master
          - zone transfer has failed
            - no IP packets between secondary and primary server(s)
              - [UDP,TCP]/53 is blocked
            - configuration errors
              - configuration errors on master server
                - ACL on zone transfer is wrong
                - TSIG key changed
              - configuration errors on slave server
                - master has changed IP address and slave is not updated
                - TSIG key changed
    - Data from false recursive resolver
      - wrong recursive resolver in resolver configuration
        - DHCP error
        - manual configuration error
      - packet injected in udp stream
        - computer beside resolver is hijacked
        - querying computer is ddos:ed with wrong data