MINISTRY OF INFORMATION AND COMUNICATIONS
VIETNAM INTERNET NETWORK INFORMATION CENTER

DNS OPERATIONS

Nguyen Trung Kien | VNNIC | 25-08-2017

www.vnnic.vn

DNS QUERY
ROOT DNS SERVER
TLD DNS SERVER
PC
LOCAL DNS SERVER
AUTHORATIVE DNS SERVER
1
2
3
4
5
6
7
8

dns
technology
internet
network
domain
router
concept
person
global
data
client
protocol
http
site
computer
database
proxy
development
hyperlink
laptop
communication
analysis
web
business
presentation
expert
pointing
websurfing
information
developer
desktop
physical
surfing
solution
service
world
media
code
website
connection
wireless
ecommerce
www
online
address
search
ftp
fiber
digital

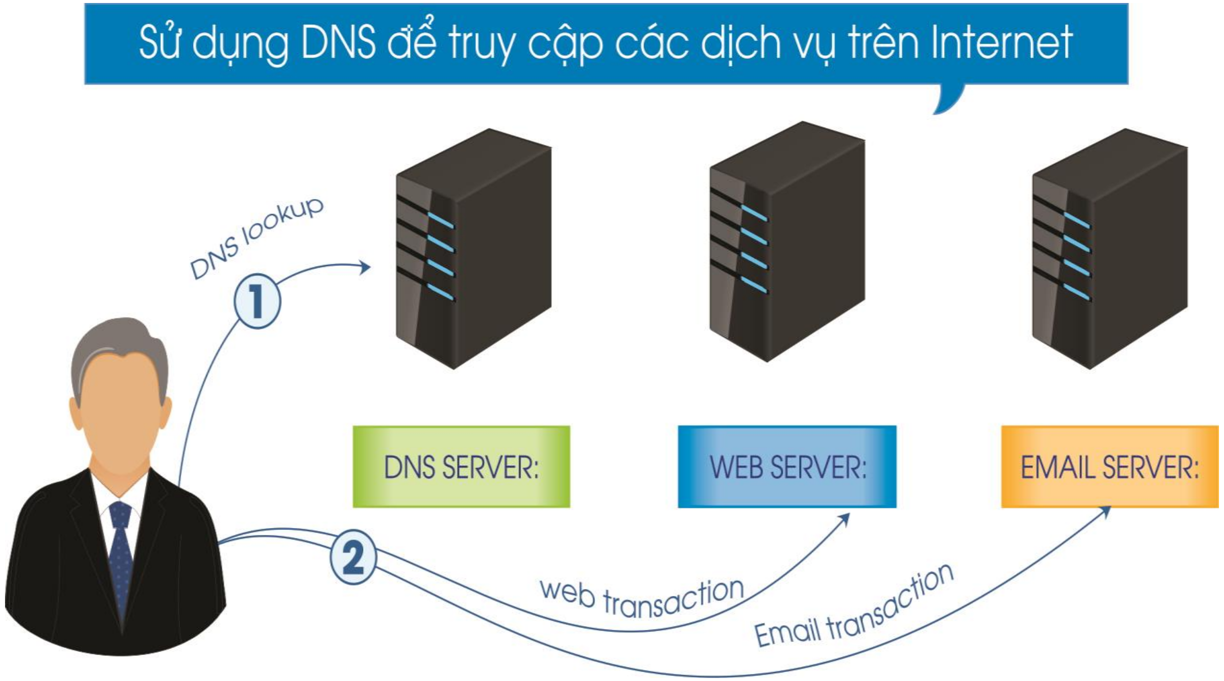
DNS

- DNS (Domain Name System): Convert names to IP addresses and back.

- DNS is hierarchical

- DNS administration is shared – no single central entity administrates all DNS data

- Protocol: TCP/UDP/53.



Authoritative server

- Authoritative servers typically only answer queries for data over which they have authority.
- Gives answers for specific zones
- Only respond to queries for these zones
- Never ask other DNS servers anything
- A server can be authoritative for >1 zone
- A zone should have >1 authoritative server

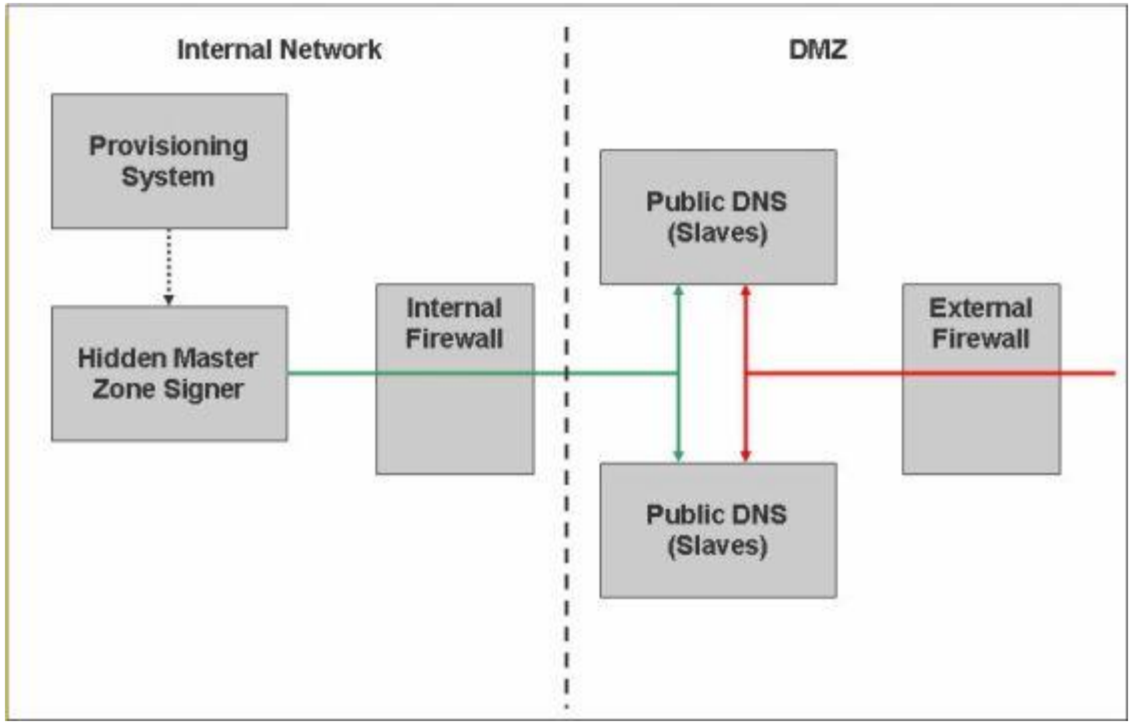
Caching server

- Receives queries from clients
- Send queries to authoritative servers
- Cache answers for later
- The TTL of the answer is used to determine how long it may be cached without re-querying.

Server Function	Information	Target audience
Authoritative	Your domains	The Internet
Recursive	All other domains	Your users

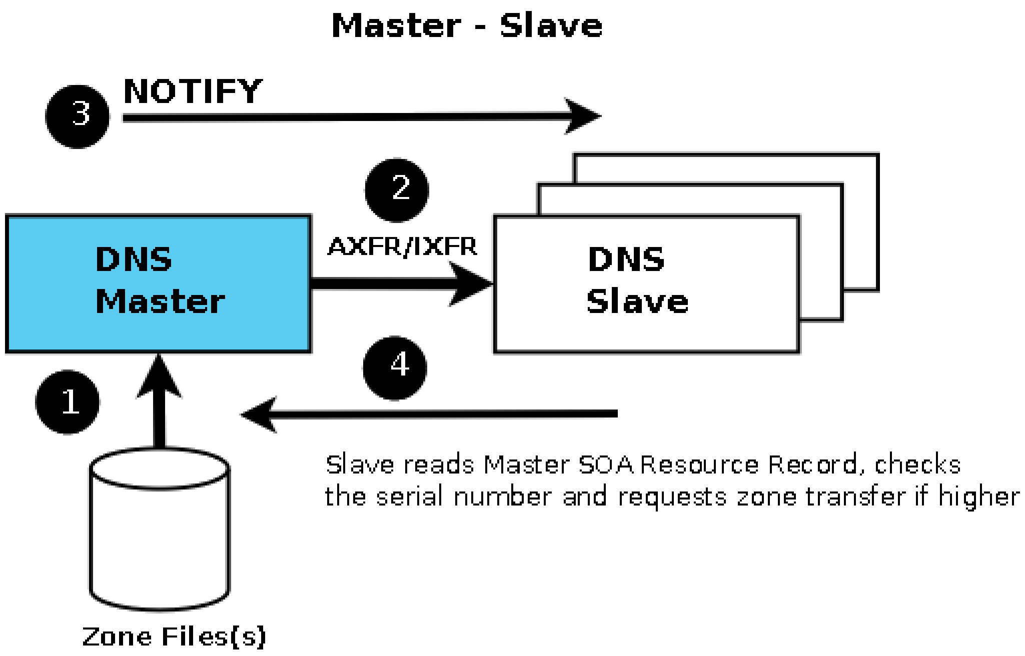
Hidden Primary DNS

- Master name server inside for zones.
- Doesn't appear in the NS records for its zones.
- Doesn't serve any resolvers.
- Only responsibility is to serve zone transfers to slave name servers



DNS Master-Slave

- Master & Slave (Primary & Secondary) are Authoritative DNS
- Slave DNS gets its zone data using a zone transfer operation
- Recommend:
  - Many Slave DNS for zones (>1)
  - Only Slave DNS serve clients
  - Implement Slave DNS for multi-site



Slave reads Master SOA Resource Record, checks the serial number and requests zone transfer if higher

Logging Information

- Have a look at the system logs.
- Check the config as well as the actual logs.
- Logging for:
    - Update
    - Queries
    - Debug
    - Security

Dualstack IPv4/IPv6

- DNS servers have both IPv4 & IPv6 addresses.
- Response to clients on IPv4/ IPv6 network.
- Typically the AAAA record gets resolved first, then the A record.
- .VN DNS servers:

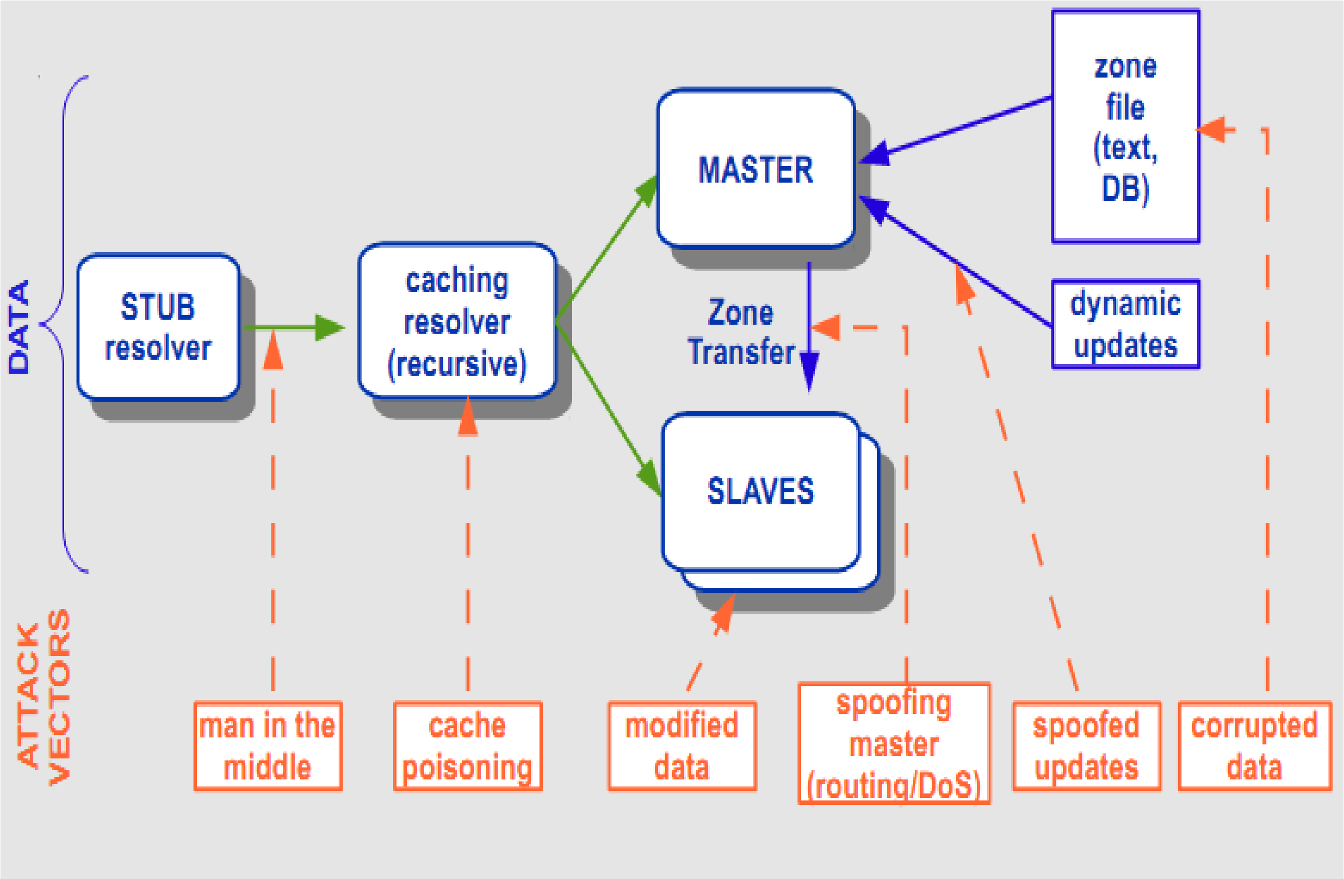
.vn DNS	IP
A.DNS-SERVERS.VN	194.0.1.18 2001:678:4::12
B.DNS-SERVERS.VN	203.119.73.105 2001:dc8:1:2::105
C.DNS-SERVERS.VN	203.119.38.105 2001:dc8:c000:7::105
D.DNS-SERVERS.VN	203.119.44.105
E.DNS-SERVERS.VN	203.119.60.105
F.DNS-SERVERS.VN	203.119.68.105 2001:dc8:d000:2::105
G.DNS-SERVERS.VN	204.61.216.115 2001:500:14:6115:ad::1

Backup/Restore

- Very important!
- DNS Server may be down, may crash, may become overloaded an stop processing queries.
- Backup DNS configs, DNS data… and store in many place.
- Deploy backup name server so that if fails, they’ll move on.

Threats to DNS

- Denial of service attacks
- Reflection/amplification attacks
- Cache poisoning
- Information disclosure
- Human error
- Hardware/software failure

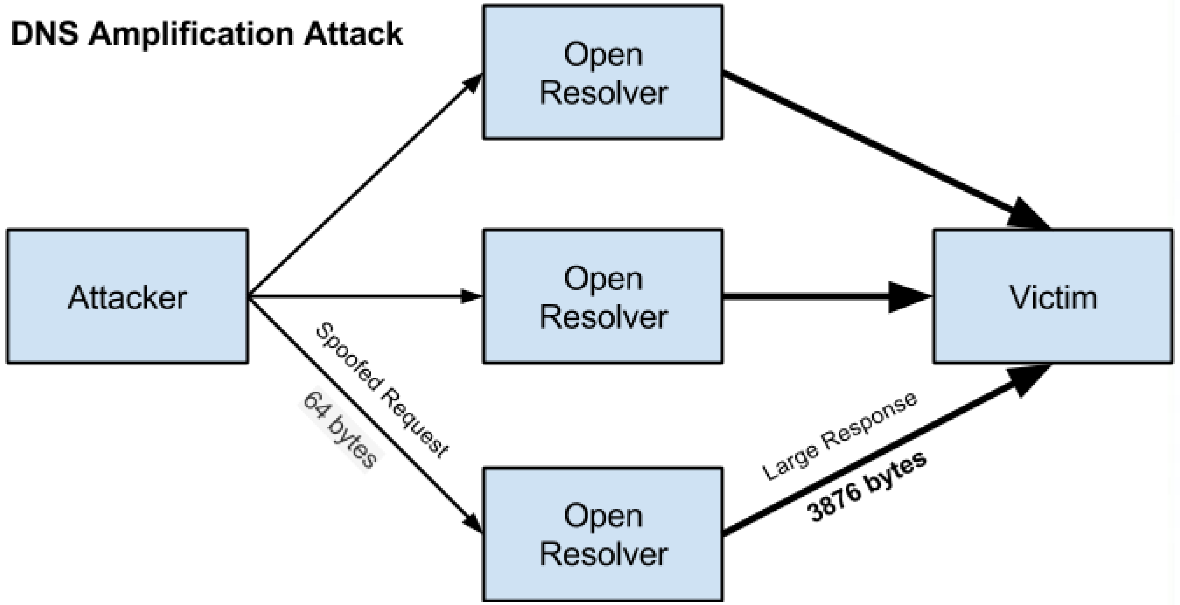


DoS attacks

- When DNS servers are the target of a DoS attack:
  - Can't resolve domains
  - May not be connected to the Internet
- Authoritative or Caching servers may be attacked
- Recommend:
  - Having multiple servers (ditributed globally)
  - Rate Limiting
  - Anycast a good technique to absorb DoS
  - Use commercial anycast services

Amplification attacks

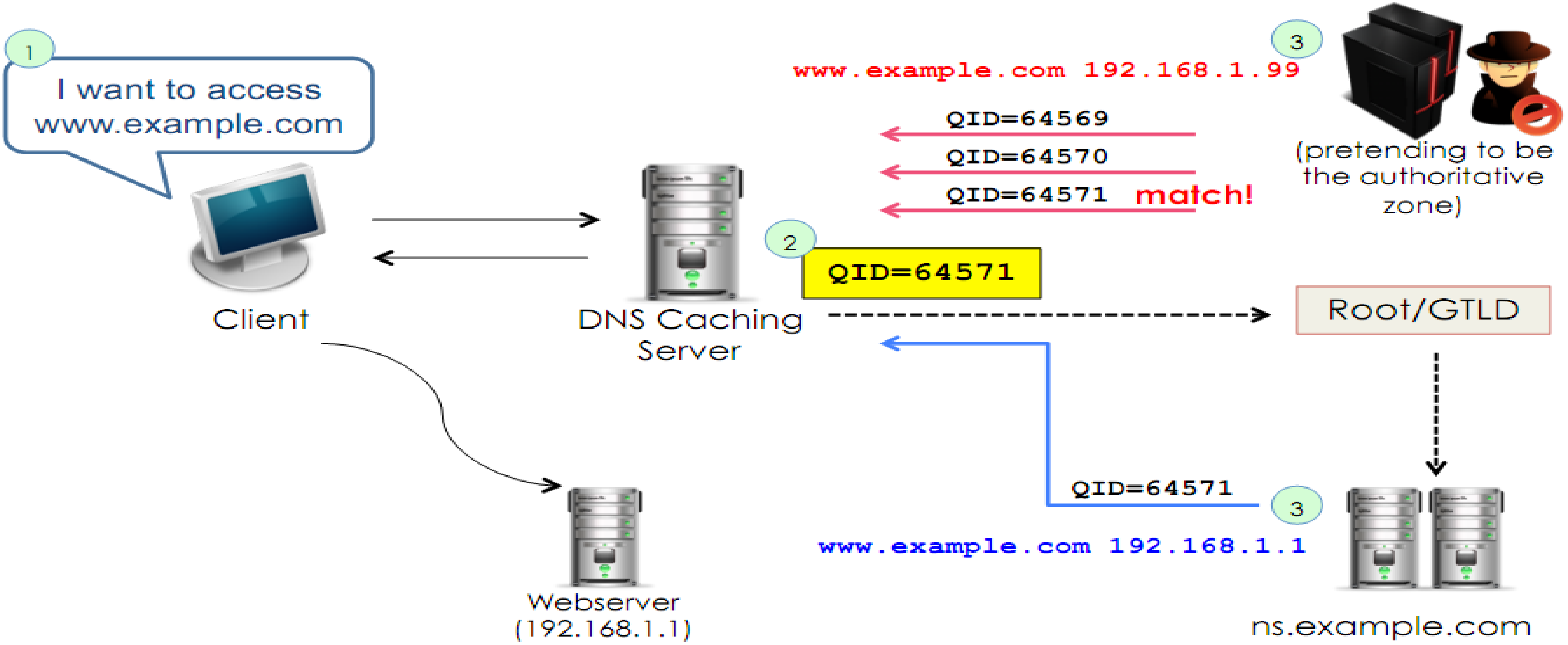
- Amplification or Reflection attack:
  - Standard DDoS mitigation technique
  - DNS servers used as tools in the attack
  - Queries with spoofed source addresses sent to DNS servers
- Server replies to the "source" with packet many times larger than the request
- Victims see lots of UDP source 53 traffic from many different source addresses.



Amplification attacks

- Tempting to limit DNS packets by size
  - Maybe breaks DNSSEC
- Don’t run open recursive servers:
  - Drop queries that are not from customers
  - Authoritative servers used in attacks too
- Rate Limiting by source IP address.
- Reference: BCP 38, BCP 140

DNS Cache Poisoning


1
I want to access www.example.com
Client
DNS Caching Server
2
QID=64571
Webserver (192.168.1.1)
www.example.com 192.168.1.99
QID=64569
QID=64570
QID=64571
match!
3
(pretending to be the authoritative zone)
Root/GTLD
QID=64571
3
www.example.com 192.168.1.1
ns.example.com

DNS Cache Poisoning

- Many tweaks to make poisoning harder
  - Being careful about processing responses
  - Transaction ID randomisation
  - Source port randomisation
- DNSSEC is the only true way to avoid it

DNSSEC

Information disclosure

- DNS is clear text
  - DNSSEC provides authentication
  - Not confidentiality
- Zone transfers
  - Allow the entire contents of a zone to be read
  - Easier for an attacker to find targets
  - Use TSIG for zone transfer !

Separation of duties

- Authoritative and recursive separated
  - Scale each service independently
  - Failure of one does not affect the other
  - Easier control
  - Easier troubleshooting
- Not confusing authoritative and cached data

Protecting authoritative servers

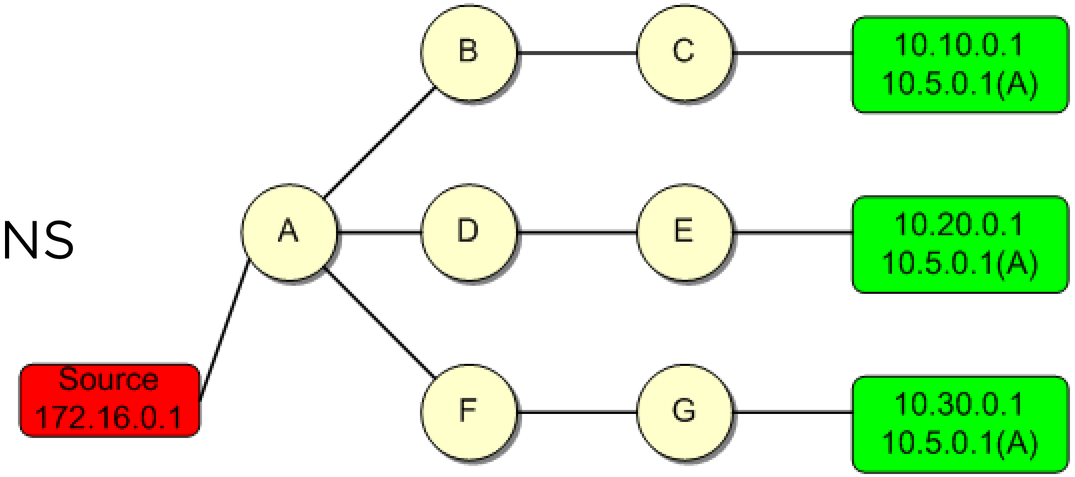
- Disable recursion.
- UDP/TCP dest port 53 from everywhere
- No other services on the same servers
- Run multiple authoritative servers
  - BCP: RFC 2182
  - Secondary service with another operator/ commercial DNS hosting services

Protecting caching servers

- Only permit queries from your customers
- Stateless packet filter
  - Permit UDP/TCP dest port 53 from customers
  - Server firewall (iptables/ipfw)
  - ACL deployed to router/switch
  - ACL deployed on dns server software

Anycast

- Routing solution
- Same prefix announced from >1 location
- Client reaches "nearest" instance
  - Based on network topology
  - BGP path selection
- Works well with short-lived sessions like DNS
- Load balancing
- Failover
- Distributed sinking of DDoS traffic
- Minimise impact of cache poisoning



Diversification

- Different location
- Different network
- Different hardware
- Different OS
- Different DNS software
- Reduced chance of total service failure
- Increased configuration complexity

Monitoring

- Check that server responds to queries
- Check that important records still exist
- DNS failure may impact alarming
  - Out-of-band alerting
- DNS monitoring from outside (ISP…)
- Network delay
- DNS service response time

Monitoring logs

- Use a tool to analyse DNS logs
    - Elastic search
    - Nagios
- Alarm on important messages
    - zone syntax errors
    - zone transfer errors
    - DNSSEC validation errors
    - Check log debug/errors

  …
- Log central.

External tools

- http://dnsviz.net/
- http://dnscheck.ripe.net/
- http://www.kloth.net/services/nslookup.php
- http://dnscheck.iis.se/
- Reference document:
  - DNS Best Practices, Mike Jager, NSRC
  - BIND Best Practices, Eddy Winstead, ISC
  -

Contact

- VNNIC DNS Support.
- Email: dns-support@vnnic.vn
- Tel: +84-24-35564944 (Ext: 600)

Thank you