Ch 5: Prevention, Protection and Mitigation of DNS Service Disruption

Updated 9-14-23

Prevention of DNS Service Disruption

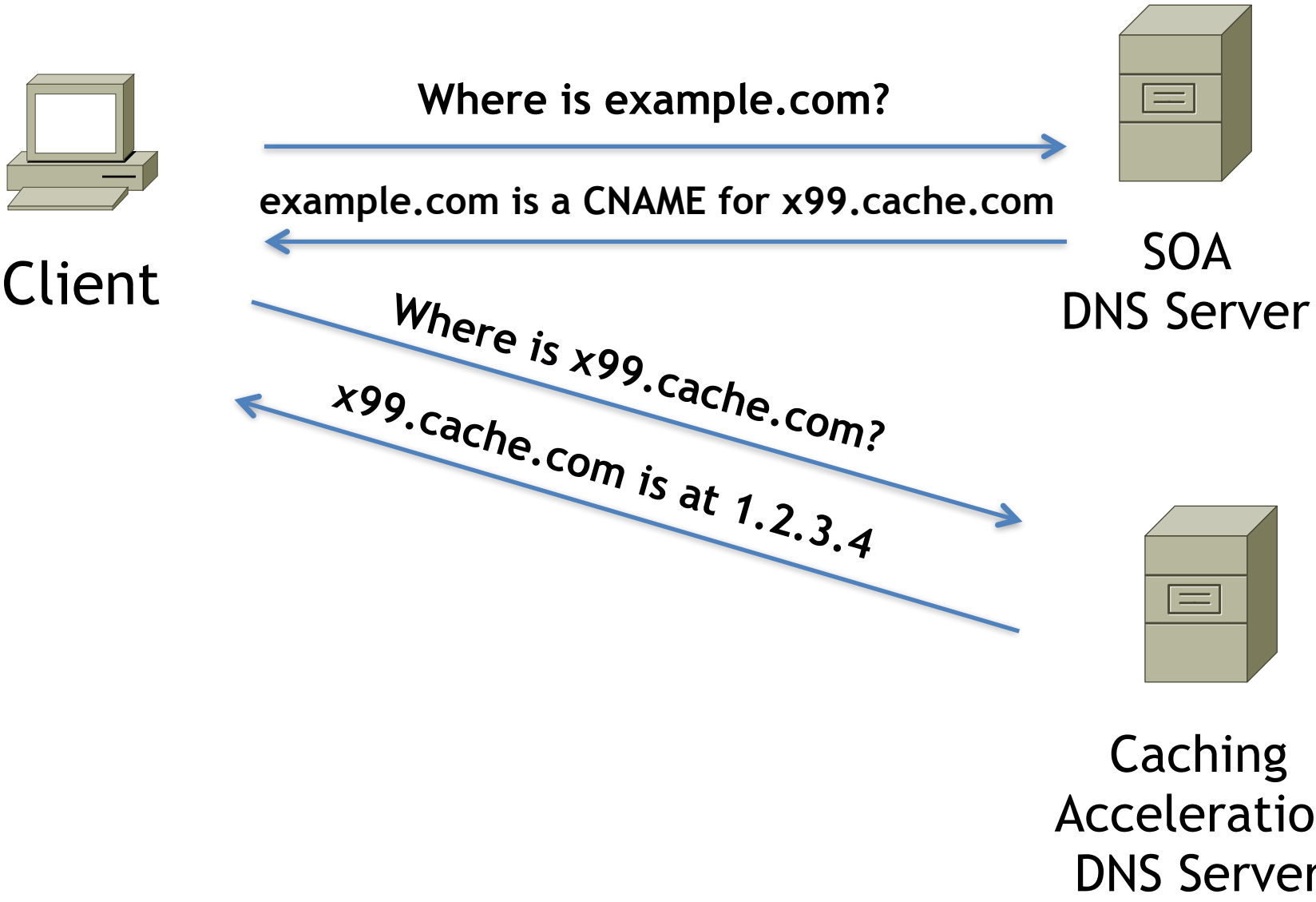
Architecture to Resist DoS

- Authoritative servers typically need to accept queries from every device on the Internet
- A **network distributed** system places authoritative servers in multiple networks
  - Small scale: different subnets with different gateways
  - Large scale: different Autonomous Systems (AS)
- **Geographically distributed** systems are in different regions or countries

Types of DoS Protection

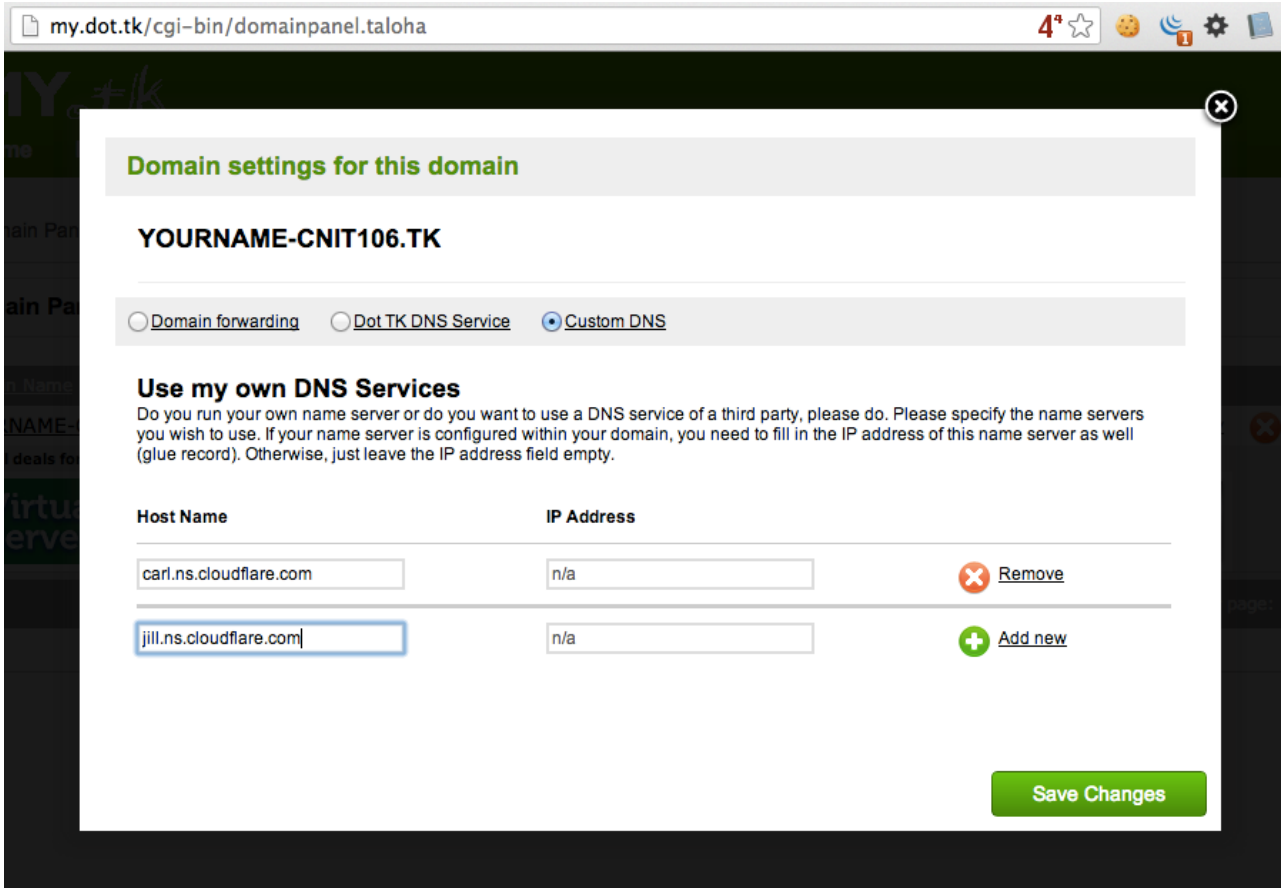
- Host authoritative DNS servers at an ISP or Content Distribution Network (CDN)
- Purchase **caching acceleration** service and delegate DNS resolution with a CNAME record
  - Risky because the authoritative server is still needed to provide the CNAME record
- Direct delegation from the TLD to the ISP's or CDN's authoritative servers
  - Better, like Cloudflare

Caching Acceleration



Project 6x

- Protecting a domain with Cloudflare



Anycast

- Multiple geographically separated servers use the same IP address
- This spreads attacks over the whole network
- Used by the root DNS servers and Cloudflare

NS Delegation

```
Sams-MacBook-Air-2:~ sambowne$ dig samsclass.info ns

; <<>> DiG 9.8.3-P1 <<>> samsclass.info ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49815
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;samsclass.info.                        IN      NS

;; ANSWER SECTION:
samsclass.info.         21600   IN      NS      tom.ns.cloudflare.com.
samsclass.info.         21600   IN      NS      coco.ns.cloudflare.com.
```

Partially Hidden Authoritative Servers

- Some of the authoritative servers are placed behind the firewalls of large ISPs or other organizations
- They act as SOA for only the users of the private network
  - Using BGP to make them preferred
- They are slave servers, updated from the master servers
- This is how UltraDNS works

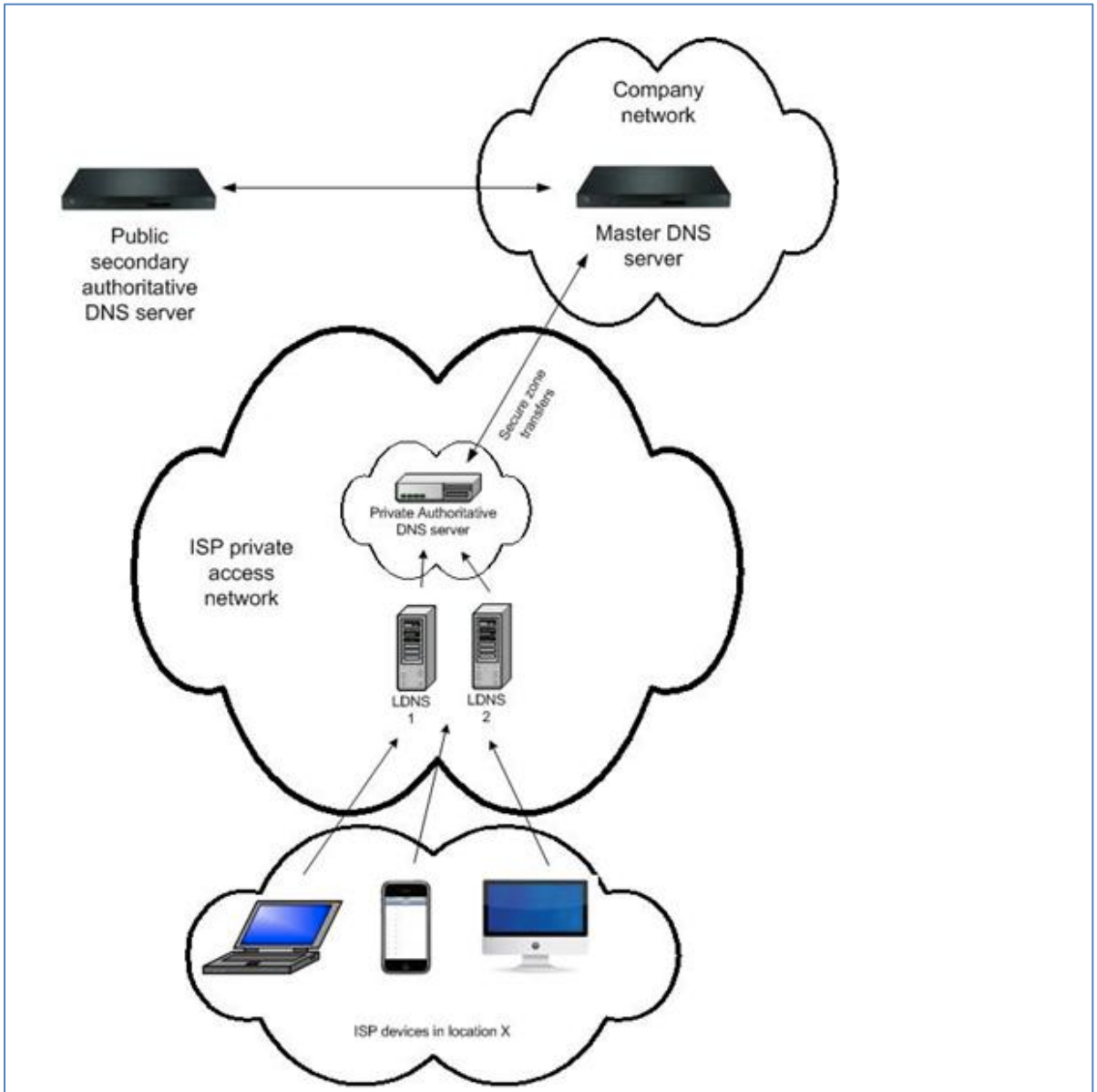


Figure 48: Placement of authoritative servers in the private access network of an ISP to protect DNS authoritative service from DoS attacks.

UltraDNS DNS Shield

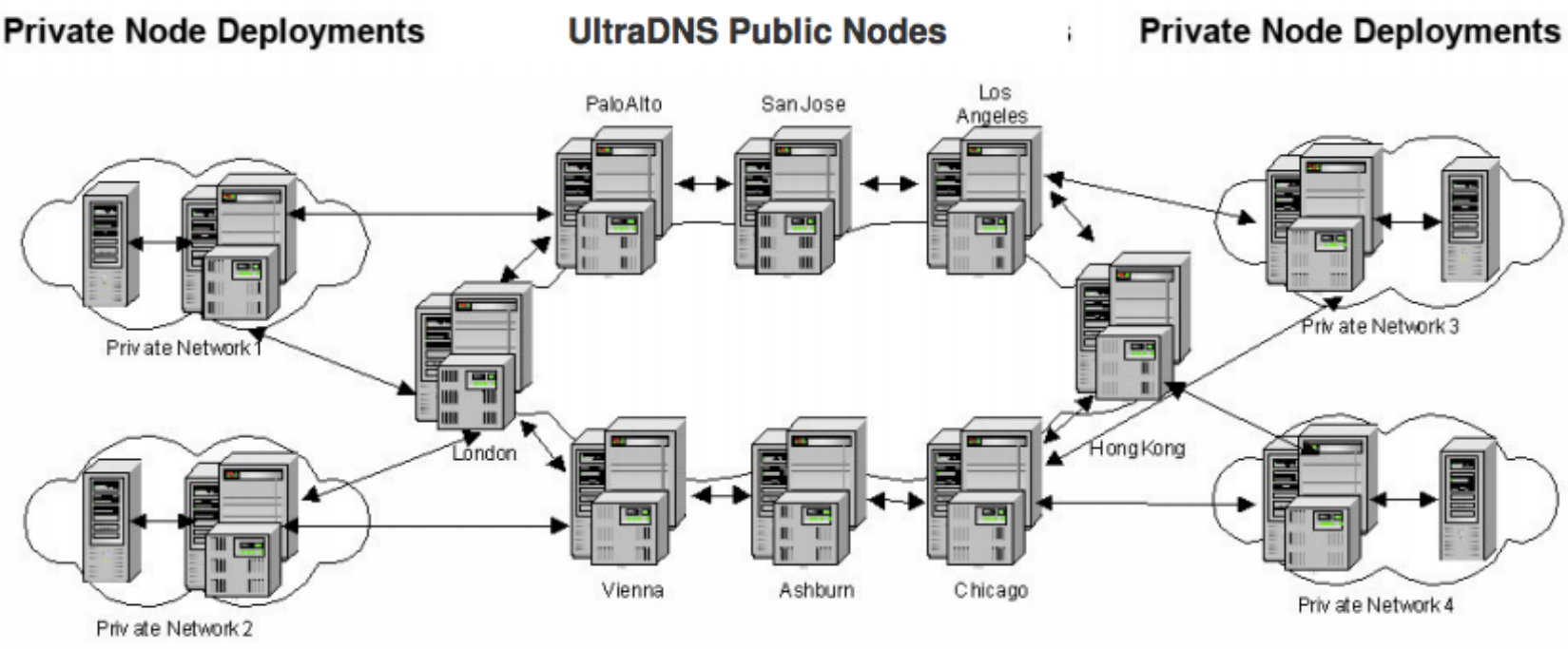


Figure 1 The DNS Shield

- Link Ch 5a

Software

- Whatever you use, keep it updated
- Bind
  - The standard
- djbdns
  - Intended to be more secure than bind, but no longer centrally maintained (links Ch 5b)
- There are many others (link Ch 5c)

DNS Security Extensions
DNSSEC

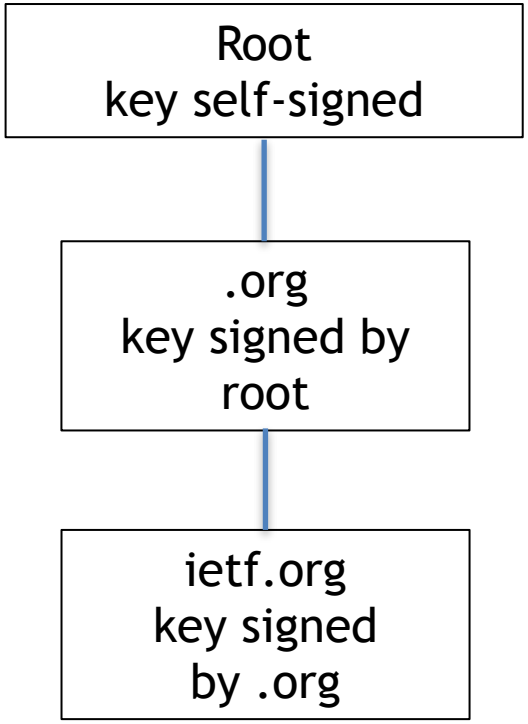
Purpose of DNSSEC

- Ensure **authenticity** of data origin
- And **integrity** of data received by a resolver from an authoritative DNS server
- Done by signing Resource Record (RR) sets
  - With a private key
  - And including the signature (RRSIG) with the record

Chain of Trust

- Resolver can verify the RRSIG with the server's Public Key
  - Published by the server in its zone file (DNSKEY)
  - Vouched for by the parent zone
  - Vouched for by its parent...
  - Unbroken chain of trust up to the root zone
- Only works if all higher-level zones are signed

DNSSEC Chain of Trust



Detailed Chain of Trust

Owner name	Record type	Zone
www.example.net.	A	example.net.
www.example.net.	RRSIG	example.net.
example.net.	DNSKEY	example.net.
example.net.	DS	net.
example.net.	RRSIG	net.
net.	DNSKEY	net.
net.	DS	.
net.	RRSIG	.
.	DNSKEY	.

- DS record contains a summary of the DNSKEY record of a child zone
- Link Ch 5d

Root Signed in 2010

» **July 15, 2010:** ICANN publishes the root zone trust anchor and root operators begin to serve the signed root zone with actual keys – **The signed root zone is available.**

- Link Ch 5e

Demonstration

- dig rrsig .
- dig dnskey .
  - Shows RRSIG and DNSKEY records for the root
- dig ds org.
- dig dnskey org.
- dig rrsig org.
- dig dnskey ietf.org
- dig rrsig ietf.org

Root RRSIG Records

```
Sams-MacBook-Pro-3:~ sambowne$ dig rrsig .

; <<>> DiG 9.10.6 <<>> rrsig .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51794
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      RRSIG

;; ANSWER SECTION:
.                       31952   IN      RRSIG   SOA 8 0 86400 20181127050000 20181114040000
2134 . 1Y9+ozV9xtCKwSgcQxneZOXSFB3wCCqs3f2mO1FwjflXhX/ysJSSyH67 rcGLMXhsktBwH1diWdRq/XdtSdr5
DgeD8uBI+/Dxh/FA2voUkLowCWpI 6zNaR3Wl/03LYDhNgKe+7fZ0TWmn5CT87ZatVpPbufjZkQx+xt2wKl+2 V3CIgB
gnflFLmcPFqZxRkPNcRZIOVo3qMHnxwRppVATn7txkHWUXwt2I O76SmYqx2GMG3mLd0BG23FNAB9AkLoHT6A6fBBG4n
4KrIEdZjb7n0RRF qRVjnL/cPHvZPkmUGcSP8XmoWwaP3S0/qebW/9n56h3GfosGc8KMgrnp L5SvGw==
.                       108002  IN      RRSIG   NS 8 0 518400 20181127180000 20181114170000
2134 . NYFQ8mFyNMhLqFGEfYK3DTs9pbWDBvlQnl6oLV0H4I0YsAZZYgRG0hew hz/9Ggskl1VYtU1qvyCWq5aRh3iG
IVQDWKzZgSQSOw/i+gzrFYnHhihT px28rpqiFDqKXBi/gBMeAToUc715KFlfyQ4si8zMA/oB35HuQoyzhA4k JFTs67
LiPkmDVg7KTMc56IADadHws50oHdZlEdWz0otUnpSRbF5Zpsz3 99iIOm+5p4nmdMyS7sE62VbD9KVfZnWlfrBJQ/ib8
yhlwroKSbzVdu5W ytnPSl25EJ0/KrM/51QRgnEYqkipz36GB+zMpdFjKCe19ixiMnMIwz11 zafMrg==

;; Query time: 223 msec
;; SERVER: 172.20.10.1#53(172.20.10.1)
;; WHEN: Wed Nov 14 16:34:13 PST 2018
;; MSG SIZE  rcvd: 600
```

Root DNSKEY Records

```
Sams-MacBook-Pro-3:~ sambowne$ dig dnskey .

; <<>> DiG 9.10.6 <<>> dnskey .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50178
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      DNSKEY

;; ANSWER SECTION:
.                       108002  IN      DNSKEY  257 3 8 AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1
vkIbzxeF3 +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8
PzgCmr3EgVLrjyBxWezF 0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e oZG+SrDK6nWeL3c6H5Apxz7Lj
Vc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN R1AkUTV74bU=
.                       108002  IN      DNSKEY  256 3 8 AwEAAdp440E6Mz7c+Vl4sPd0lTv2Qnc85dTW64j0RDD7sS/
zwxWDJ3QR ES2VKDO0OXLMqVJSs2YCCSDKuZXpDPuf++YfAu0j7lzYYdWTGwyNZhEa XtMQJIKYB96pW6cRkiG2Dn8S2vvo/PxW9PKQ
syLbtd8PcwWglHgReBVp 7kEv/Dd+3b3YMukt4jnWgDUddAySg558Zld+c9eGWkgWoOiuhg4rQRkF stMX1pRyOSHcZuH38o1WcsT4y
3eT0U/SR6TOSLIB/8Ftirux/h297oS7 tCcwSPt0wwry5OFNTlfMo8v7WGurogfk8hPipf7TTKHIi20LWen5RCsv YsQBkYGpF78=
.                       108002  IN      DNSKEY  257 3 8 AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSE
W0O8gcCjF FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL49
6M/QZxkjf5/Efucp2gaD X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz W5hOA2hzCTMjJPJ8LbqF6dsV6
DoBQzgul0sGIcGOYl7OyQdXfZ57relS Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0=

;; Query time: 436 msec
;; SERVER: 172.20.10.1#53(172.20.10.1)
;; WHEN: Wed Nov 14 16:35:34 PST 2018
;; MSG SIZE  rcvd: 853
```

Top-Level Domain: org.

```
Sams-MacBook-Pro-3:~ sambowne$ dig +short ds org.
9795 7 1 364DFAB3DAF254CAB477B5675B10766DDAA24982
9795 7 2 3922B31B6F3A4EA92B19EB7B52120F031FD8E05FF0B03BAFCF9F891B FE7FF8E5
Sams-MacBook-Pro-3:~ sambowne$ dig +short dnskey org.
256 3 7 AwEAAcLdAPt3vn/ND00zZlyTx7OBko+9YeCrSl2eGuEXjef0Lqf0tKGi koHwnmTHtT8J/aGqkZImLMVByJbknE0wKDnbvb
KDoTQxPwUQZLH6k3sT dsPKESKDSBSc6VFMq35gx6CeuRYZ9KkGWiUsKqJhXPo6tyJFCBxfaNQQ yrzBnv4/
257 3 7 AwEAAZTjbIO5kIpxWUtyXc8avsKyHIIZ+LjC2Dv8naO+Tz6X2fqzDC1b dq7HlZwtkaqTkMVVJ+8gE9FIreGJ4c8G1GdbjQ
gbP1OyYIG7OHTc4hv5 T2NlyWr6k6QFz98Q4zwFIGTFVvwBhmrMDYsOTtXakK6QwHovA1+83BsU ACxlidpwB0hQacbD6x+I2RCDzYu
Tzj64Jv0/9XsX6AYV3ebcgn4hL1jI R2eJYyXlrAoWxdzxcW//5yeL5RVWuhRxejmnSVnCuxkfS4AQ485KH2tp dbWcCopLJZs6tw8q
3jWcpTGzdh/v3xdYfNpQNcPImFlxAun3BtORPA2r 8ti6MNoJEHU=
257 3 7 AwEAAcMnWBKLuvG/LwnPVykcmpvnntwxfshHlHRhlY0F3oz8AMcuF8gw 9McCw+BoC2YxWaiTpNPuxjSNhUlBtcJmcdkz3/
r7PIn0oDf14ept1Y9p dPh8SbIBIWx50ZPfVRlj8oQXv2Y6yKiQik7bi3MT37zMRU2kw2oy3cgr sGAzGN4s/C6SFYon5N1Q2O4hGDb
eOq538kATOy0GFELjuauV9guX/431 msYu4Rgb5lLuQ3Mx5FSIxXpI/RaAn2mhM4nEZ/5IeRPKZVGydcuLBS8G ZlxW4qbb8MgRZ8bw
Mg0pqWRHmhirGmJIt3UuzvN1pSFBfX7ysI9PPhSn wXCNDXk0kk0=
256 3 7 AwEAAXxsMmN/JgpEE9Y4uFNRJm7Q9GBwmEYUCsCxuKlgBU9WrQEFRrvA eMamUBeX4SE8s3V/TEk/TgGmPPp0pMkKD7msel
uK6Ard2HZ6O3nPAzL4 i8py/UDRUmYNSCxwfdfjUWRmcB9H+NKWMsJoDhAkLFqg5HS7f0j4Vb99 Wac24Fk7
Sams-MacBook-Pro-3:~ sambowne$ dig +short rrsig org.
DS 8 1 86400 20181127180000 20181114170000 2134 . t8HmqYoIRhF3XUZ0STEA9kvqmShpgDxUVhEjg0GQvKNcWQZkaT1LI
Lv2 qZXitJ8vvB4FcxJkwewHf6sKgliwcy5W+LZsPJ6BItaX3a47DZvE53t9 +kSf3oN/7HSkWxKpWEW9Ydn2nAtQCmwHZm2hURoLD9
Q8Z9So4DZf1G8l Lcwg2WetbEPkG544UMc36taCCyHVsds8N3hqDnx4YsrM0JHeoNVRGJhN 8O9h3zIqlVztoEEgGzt++wb/AuhG6sV
qHf5qQ2O3+aUWraFmgJpMS6UF Hc2ywti8dFUQXIFlOFEnbvLLy+y3q0fveKWUzZkPWcjoKUdgAuBOPsZ7 TYhw7w==
NS 7 1 86400 20181130152943 20181109142943 6368 org. sxxjxmA4CljzwkLIghDhyKg1/TntId5+4B6y872lF+y//vHnJz
70VCtX 0lN4/Bws2mjqO+XsH8AKmy6KRQs/LDwNdsEw+QIfnr+m946PMwDakqIX A68/UGZJWMCAgFRYPMIAYoxMbAOOhnEjV9Ykv1a
rGjnOGUEU8pYC0EUx h3Y=
Sams-MacBook-Pro-3:~ sambowne$
```

DNSSEC of Top-Level Domains

Nov. 2013

- 332 TLDs in the root zone in total
- 135 TLDs are signed;
- 129 TLDs have trust anchors published as DS records in the root zone;
- 3 TLDs have trust anchors published in the ISC DLV Repository.

Nov. 2016

- 1509 TLDs in the root zone in total
- 1360 TLDs are signed;
- 1349 TLDs have trust anchors published as DS records in the root zone;
- 5 TLDs have trust anchors published in the ISC DLV Repository.

Nov. 2018

Link Ch 5f

- 1535 TLDs in the root zone in total
- 1400 TLDs are signed;
- 1391 TLDs have trust anchors published as DS records in the root zone;
- 0 TLDs have trust anchors published in the ISC DLV Repository.

- " Is DNSSEC a good idea? Or is it nothing more than a whole lot of effort with little in the way of tangible benefit? Why aren't `www.google.com`, `www.amazon.com` or `www.microsoft.com` DNSSEC signed? Or, if we turn to retail banks, then why aren't `www.bankofamerica.com`, `www.hsbc.com` or `www.bnpparibas.com` DNSSEC-signed?"
- https://blog.apnic.net/2023/02/20/opinion-to-dnssec-or-not/


DNSSEC Is Dead, Stick a Fork in It
By: Larry Seltzer | December 16, 2007
Opinion: If political battles weren't preventing DNSSEC from being used seriously on the Internet, we'd have to deal with the fact that the major resolvers would reject it and that technical problems would make it unsatisfying.

- Link Ch 5n

Cloudflare Looks to Take the Pain Out of DNSSEC Protocol Adoption

Larry Loeb, Author, 9/21/2018

Email This Print Comment

Login

50% 50%

Cloudflare is adding a new feature to its hosting and firewall products that the networking company hopes will address the slow uptake of the Domain Name System Security Extensions (DNSSEC) protocol.

The method to support the DNSSEC protocol has been a manual one before this, requiring a website owner to add a "DS record" to its account with their registrar.

A Cloudflare customer that is working with a registry that supports DNSSEC can activate it for their account by the press of a button from the Cloudflare dashboard.

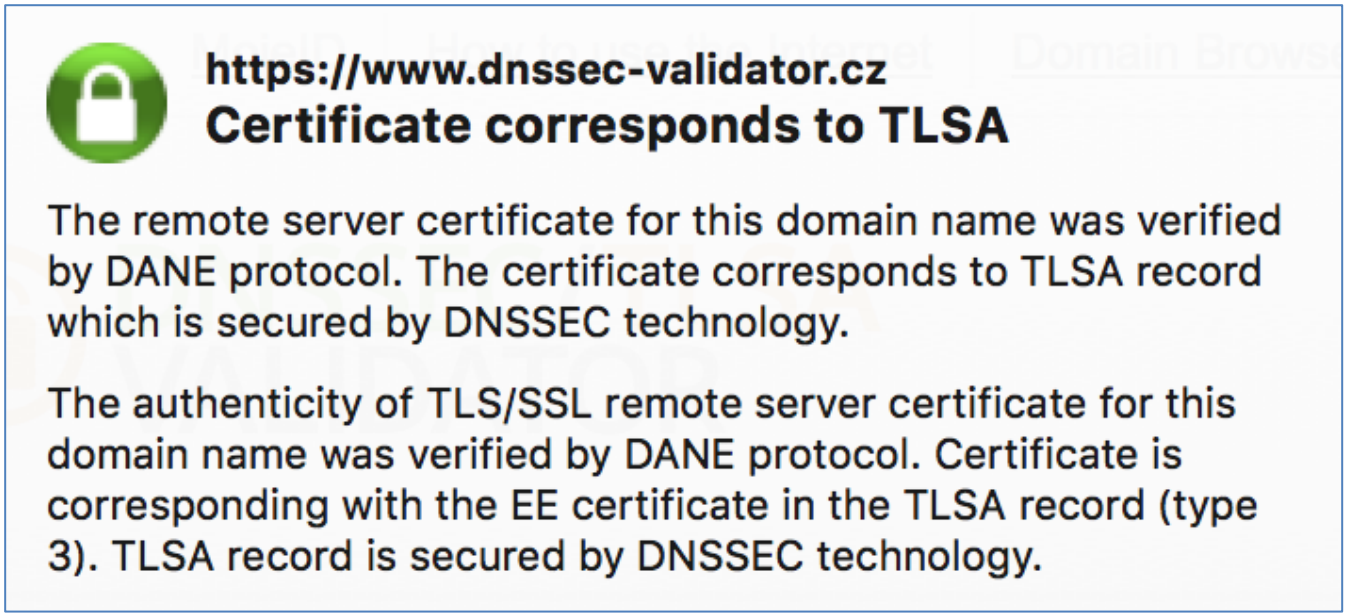
- Link Ch 5o

DNSSEC Validator Browser Extension

- Link Ch 5j

DNS-based Authentication of Named Entities (DANE)

- Uses DNSSEC to validate SSL certificates, not Certificate Authorities
  - Link Ch 5k



DNSSEC Issues

- Protocol still changing
- Only secures record to resolver, not traffic from resolver to client
- Another reason to disallow external DNS servers like 8.8.8.8
  - To keep all resolver traffic local

Authenticated Denial of Existence

- There is **no** fred.ccsf.edu
  - Three systems to prove that
- NXT record (1999); insecure & replaced by
- NSEC record (2005); insecure & replaced by
- NSEC3 record (2008)
- All incompatible with one another

Transaction Signatures: TSIG

- Maintains integrity of DNS messages between two servers
- Cryptographically signs messages with TSIG
  - Calculates a Message Authentication Code
  - Encrypts it with a secret key
  - Key shared by the two end-nodes
  - Includes the time, to prevent replay attacks
  - TSIG expires after the "time fudge factor"
- You must generate secret key and securely transmit it to the other server

Transaction Signatures: TSIG

- Originally used MD5 only, but now also uses SHA-1 and SHA-256
- Error messages include BADKEY, BADSIG, and BADTIME
- Error messages are unsigned
  - They can be spoofed, resulting in DoS

Transaction Signatures: SIG(0)

- Alternative signature method using public key cryptography
- Public key stored in a KEY record

Transaction Keys (TKEY)

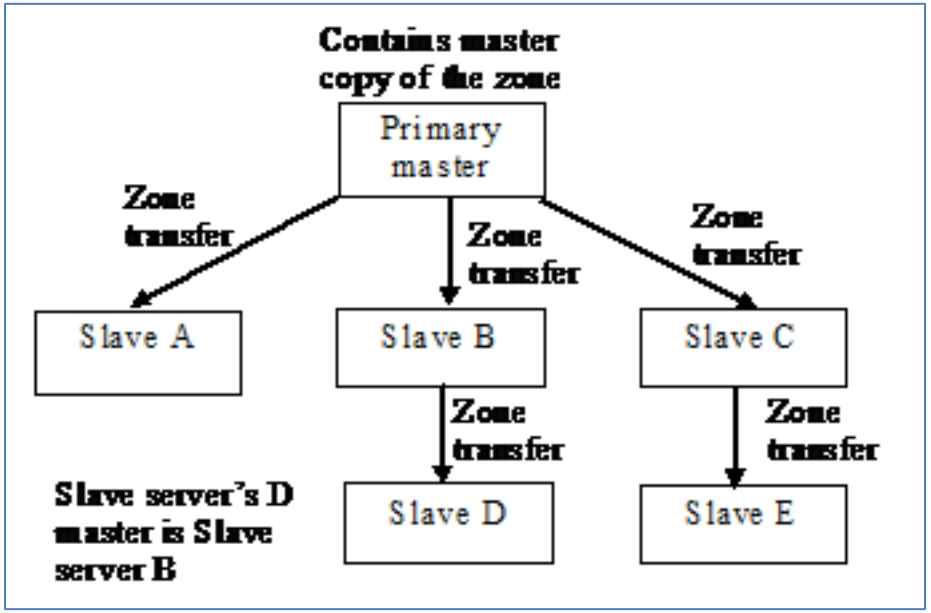
- Establishes a shared secret using
  - Diffie-Hellman key exchange, or
  - General Security Service API (based on Kerberos)
- TKEY record contains the keying material required
- Vulnerable to man-in-the-middle attacks
  - Should be secured with SIG(0) (shared secret)

Software Diversification

- Most root servers use Bind
- K and H servers use NSD from NLnetlabs

Master-Slave Setup

- Changes are made at the master
- Replicate to the slaves
- Slaves can be masters of lower-level slaves



Configuring a Slave Server in Bind

```
zone "packetproof.com" IN {
        type slave;
        file "db.packetproof.com.bk";
        masters {184.106.196.10;};
};
```

Limitation of 512 Bytes

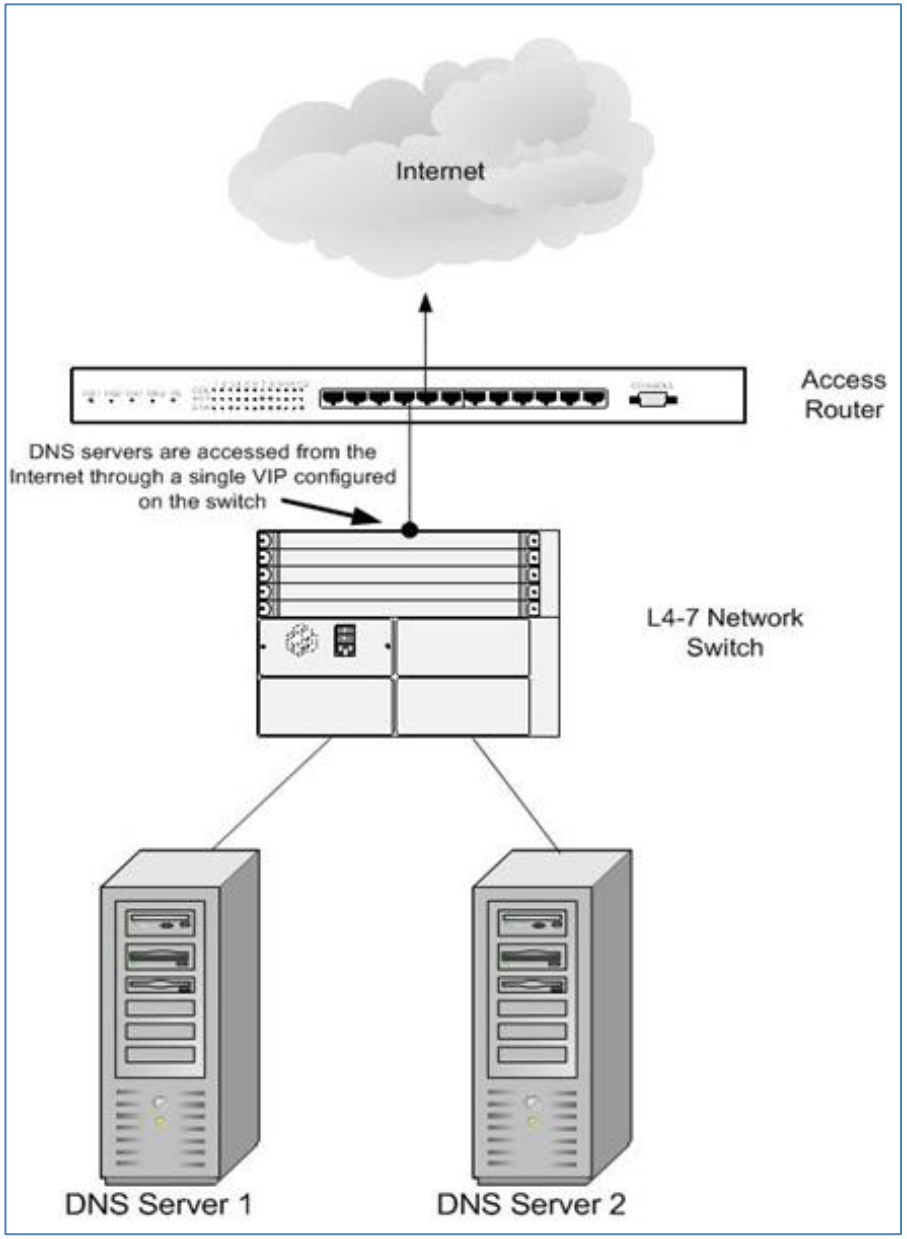
- Running many slave servers is good for fault-tolerance
  - But they all need to be listed as authoritative servers in DNS responses
  - Limited to 512 bytes in legacy systems
- Failover via multiple NS records is slow
  - Requires several seconds for timeout of a bad server

CCSF.EDU has 4 NS Records on 4-28-15

```
.  .  .  .  .  .  .  .  .  sambowne Tue Apr 28 16:27:54
~ $dig ns ccsf.edu

; <<>> DiG 9.8.3-P1 <<>> ns ccsf.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59531
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ccsf.edu.                      IN      NS

;; ANSWER SECTION:
ccsf.edu.               18342   IN      NS      ns3.ccsf.edu.
ccsf.edu.               18342   IN      NS      ns4.cenic.org.
ccsf.edu.               18342   IN      NS      ns6.cenic.org.
ccsf.edu.               18342   IN      NS      ns5.cenic.org.
```

Automatic Failover

- Use a load balancer
- Appears to be a single server to external nodes



Protection of DNS Service

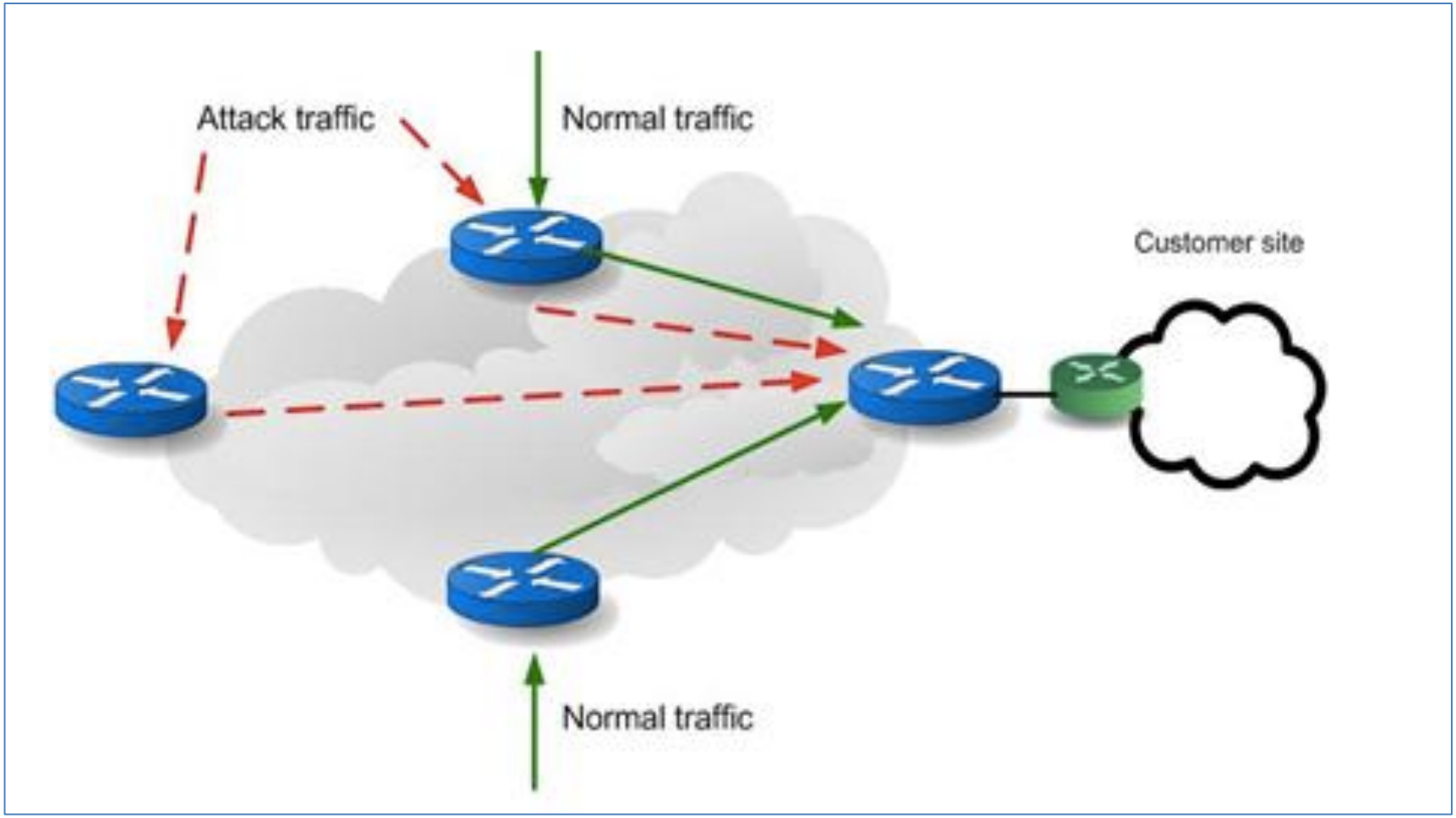
Firewalls, IDS/IPS

- Run on hardened systems
- Port 53 UDP/TCP open
- Management ports only open to internal hosts
- IDS/IPS blocks known attacks by signatures
- Firewalls limit traffic with Access Control Lists (ACLs)
- Older firewalls limit DNS packets to 512 bytes
  - Now obsolete; EDNS allows UDP packets up to 4096 bytes (link Ch 5i)

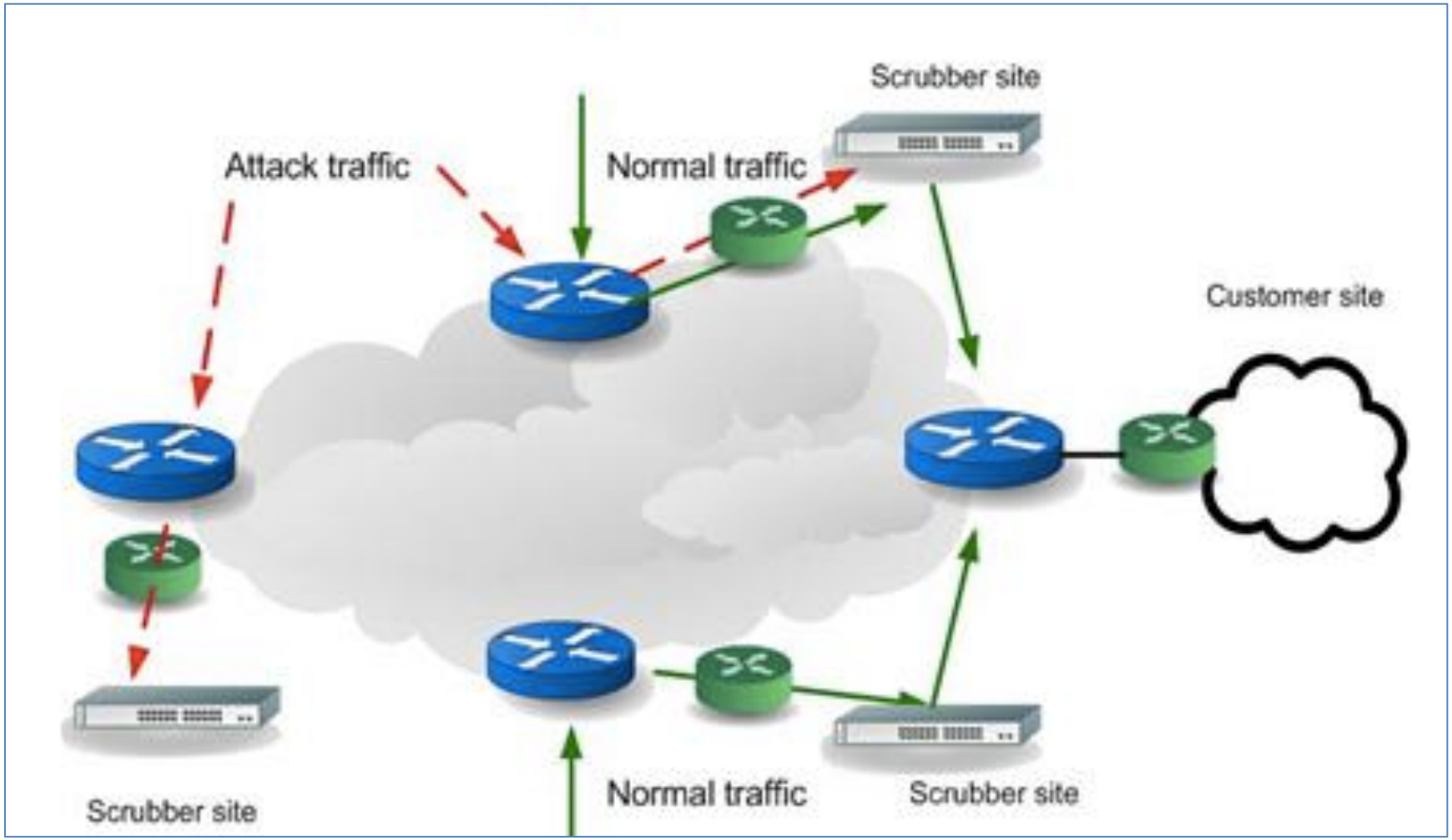
Scrubbers

- DDoS attacks look like many legitimate customers
- Scrubbers block packets that meet DDoS criteria
  - Not usually fully automated
- When under attack, BGP updates are sent to redirect traffic to the scrubbers

Normal Networking



Using Scrubbers



Service Monitoring and Restoration

Monitoring

- Send periodic probes from multiple ISPs and geographic regions
  - Such as DNS requests
  - Send directly to monitored servers
  - Verify that responses are accurate

Backups

- Regular backups of the DNS servers are essential
- Can be full or incremental
- Could back up whole OS, or just DNS configuration files
- Cloud DNS servers must be backed up too
  - Using backup tools appropriate for the cloud service
- MUST TEST YOUR BACKUPS

Slow DNS Response

- If a DNS server is down, it slows responses
- Because the dead server must time out before another server is queries
- Remove NS and A records for failed server to avoid this


Kahoot!