DNS (Domain Name System)

DNS - Background

Latar Belakang (Background) DNS

Domain Name System (DNS) diciptakan untuk memudahkan navigasi di internet. Sebelum DNS, komputer menggunakan sistem yang disebut hosts.txt, sebuah file teks yang berisi daftar nama domain dan alamat IP yang sesuai. Namun, seiring pertumbuhan internet, metode ini menjadi tidak efisien karena sulit dikelola dan diperbarui secara manual.

□□ Sejarah Singkat DNS

1. Era Awal Internet (1970-an – Awal 1980-an)
   - Komunikasi antar komputer di ARPANET (cikal bakal internet) menggunakan alamat IP numerik.
   - Sistem berbasis hosts.txt diperkenalkan oleh Stanford Research Institute (SRI) untuk menyimpan pemetaan nama dan alamat IP.
2. Penciptaan DNS (1983)
   - Paul Mockapetris merancang dan memperkenalkan DNS sebagai solusi otomatis untuk menerjemahkan nama domain ke alamat IP.
   - Sistem ini menggantikan hosts.txt dengan metode yang lebih terstruktur, terdistribusi, dan scalable.
3. Standarisasi DNS (1984 – 1987)
   - DNS diadopsi secara luas setelah diterbitkannya spesifikasi resmi dalam RFC 882 dan RFC 883 (kemudian diperbarui menjadi RFC 1034 dan RFC 1035).
   - Sistem hierarkis diperkenalkan, membagi domain menjadi beberapa tingkat seperti .com, .org, .edu, dan sebagainya.

□□ Struktur Hierarki DNS

DNS memiliki sistem berbasis hierarki, mirip dengan struktur pohon terbalik:

1. Root Level: Puncak dari sistem DNS, diwakili oleh titik (.).
2. TLD (Top-Level Domain): Seperti .com, .org, .id, .edu.
3. Second-Level Domain: Nama unik yang didaftarkan (contoh: example dalam example.com).
4. Subdomain: Bagian tambahan sebelum second-level domain (contoh: www dalam www.example.com).

□□ Tujuan Utama DNS

1. Menerjemahkan Nama Domain ke Alamat IP – Memudahkan akses ke situs web tanpa menghafal alamat numerik.

2. Mendistribusikan Beban – DNS terdesentralisasi agar dapat melayani permintaan dalam skala besar.
3. Meningkatkan Keamanan dan Kecepatan – Dengan fitur seperti caching, redundansi, dan DNS Security Extensions (DNSSEC).

□□ Pentingnya DNS dalam Internet Modern

DNS menjadi tulang punggung komunikasi internet modern, memungkinkan miliaran perangkat terhubung secara efisien dan cepat. Tanpa DNS, navigasi di internet akan sangat rumit karena pengguna harus mengingat alamat IP dari setiap layanan atau situs web yang ingin diakses.

DNS - Install Bind9

1. Persiapan

Pastikan sistem Anda diperbarui :

```
sudo apt update && sudo apt upgrade -y
```

2. Install Bind9

Jalankan perintah berikut untuk menginstal Bind9 :

```
sudo apt install bind9 bind9-utils bind9-doc -y
```

3. Konfigurasi Bind9

- Konfigurasi Utama di `named.conf.local`
  Buka file konfigurasi :

```
sudo nano /etc/bind/named.conf.local
```

Tambahkan zona untuk domain (contoh: `ilusidigital.com`) :

```
zone "ilusidigtal.com.com" {
    type master;
    file "/etc/bind/db.ilusidigital.com";
};

zone "2.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```

- Membuat Zona File Forward (`db.ilusidigital.com`)
  Salin template file:

```
sudo cp /etc/bind/db.local /etc/bind/db.ilusidigital.com
sudo nano /etc/bind/db.ilusidigital.com
```

Isi dengan konfigurasi berikut (sesuaikan `contoh.com` dan IP) :

```
$TTL    604800
@       IN      SOA     ns.ilusidigital.com. admin.ilusidigital.com. (
                        2024031901 ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL

; Records
@       IN      NS      ns.ilusidigital.com.
ns      IN      A       192.168.2.10
www     IN      A       192.168.2.20
```

- Membuat Zona File Reverse (db.192)
  Buat file reverse :

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
sudo nano /etc/bind/db.192
```

Isi dengan konfigurasi berikut :

```
$TTL    604800
@       IN      SOA     ns.ilusidigital.com. admin.ilusidigital.com. (
                        2024031901 ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL

; Records
@       IN      NS      ns.ilusidigital.com.
10      IN      PTR     ns.ilusidigital.com.
20      IN      PTR     www.ilusidigital.com.
```

4. Cek dan Validasi Konfigurasi

- Periksa Kesalahan Konfigurasi :

```
sudo named-checkconf
```

- Validasi File Zona :

```
sudo named-checkzone ilusidigital.com /etc/bind/db.ilusidigital.com
sudo named-checkzone 2.168.192.in-addr.arpa /etc/bind/db.192
```

Jika hasilnya **OK**, lanjutkan ke langkah berikutnya.

5. Restart dan Aktifkan Bind9

Restart layanan Bind9 :

```
sudo systemctl restart bind9
```

Aktifkan agar otomatis berjalan saat boot :

```
sudo systemctl enable bind9
```

6. Konfigurasi Client (Resolv.conf)

Edit file `resolv.conf` :

```
sudo nano /etc/resolv.conf
```

Tambahkan baris berikut :

```
nameserver 192.168.2.10
search ilusidigital.com
```

7. Uji Coba DNS

- Cek Nama Domain :

```
dig www.ilusidigital.com
```

- Cek Reverse DNS:

```
dig -x 192.168.2.10
```

- Cek dengan `nslookup` :

```
nslookup www.ilusidigital.com
```

Jika semua berhasil, berarti DNS Bind9 sudah berjalan dengan benar.

DNS - List Domain Name System Public

Berikut adalah daftar tabel alamat DNS publik :

Provider	Primary DNS	Secondary DNS	Kegunaan Utama	Keunggulan
Cloudflare	`1.1.1.1`	`1.0.0.1`	DNS cepat dan menjaga privasi (tanpa logging).	Cepat, privasi tinggi, mendukung DNS over HTTPS (DoH) dan DNS over TLS (DoT).
Cloudflare Family	`1.1.1.2`	`1.0.0.2`	Blokir malware.	Keamanan ekstra untuk perangkat keluarga.
Cloudflare Family	`1.1.1.3`	`1.0.0.3`	Blokir malware dan konten dewasa.	Proteksi ganda: malware + konten dewasa.
Google Public DNS	`8.8.8.8`	`8.8.4.4`	DNS cepat dan stabil untuk kebutuhan umum.	Performa tinggi, cakupan global luas.
Google Secure DNS	`2001:4860:4860::8888`	`2001:4860:4860::8844`	DNS Google dalam format IPv6.	Dukungan IPv6 untuk lingkungan modern.
Quad9 Secure	`9.9.9.9`	`149.112.112.112`	DNS aman dengan filter malware dan privasi tinggi.	Perlindungan malware, tanpa logging IP pengguna.
Quad9 Unsecured	`9.9.9.10`	`149.112.112.10`	DNS tanpa filter (tidak memblokir konten).	Resolusi DNS murni tanpa sensor.
Quad9 ECS (EDNS)	`9.9.9.11`	`149.112.112.11`	DNS aman + mendukung EDNS Client Subnet.	Cocok untuk meningkatkan kecepatan CDN.
OpenDNS (Cisco)	`208.67.222.222`	`208.67.220.220`	DNS cepat, mendukung parental control.	Stabil, fitur filter kustom (OpenDNS Home).
OpenDNS Family	`208.67.222.123`	`208.67.220.123`	Blokir konten dewasa secara otomatis.	Proteksi anak-anak dan keluarga.
AdGuard DNS	`94.140.14.14`	`94.140.15.15`	Blokir iklan dan pelacak secara otomatis.	Anti-iklan, privasi tinggi, open-source.
AdGuard Family	`94.140.14.15`	`94.140.15.16`	Blokir iklan, pelacak, dan konten dewasa.	Perlindungan tambahan untuk anak-anak.
Clean Browsing	`185.228.168.9`	`185.228.169.9`	DNS aman dengan filter konten dewasa.	Proteksi keluarga, bebas konten dewasa.

Provider	Primary DNS	Secondary DNS	Kegunaan Utama	Keunggulan
Clean Browsing Family	`185.228.168.168`	`185.228.169.168`	Blokir malware dan konten dewasa secara penuh.	Keamanan tinggi dengan kontrol ketat.
Yandex DNS	`77.88.8.8`	`77.88.8.1`	DNS cepat dengan pilihan mode proteksi.	Pilihan mode dasar, aman, atau family.
Yandex Safe	`77.88.8.88`	`77.88.8.2`	Melindungi dari malware dan phishing.	Fokus pada keamanan pengguna.
Yandex Family	`77.88.8.7`	`77.88.8.3`	Blokir konten dewasa dan malware.	Cocok untuk lingkungan rumah atau sekolah.
Comodo Secure DNS	`8.26.56.26`	`8.20.247.20`	DNS cepat dengan perlindungan dari ancaman online.	Blokir malware, phishing, dan spyware.
IBM Quad101	`101.101.101.101`	`101.102.103.104`	DNS aman, cepat, dan menjaga privasi pengguna.	Fokus pada privasi dan performa tinggi.
NextDNS	**Custom**	**Custom**	DNS berbasis kustomisasi (filter iklan, malware).	Fleksibel, analitik lengkap, open-source.
UltraDNS	`156.154.70.1`	`156.154.71.1`	DNS komersial cepat dengan perlindungan malware.	Performa tinggi, tersedia di banyak negara.

Rangkuman Penggunaan :

- **Untuk Kecepatan & Privasi Tinggi**:
  - Cloudflare (`1.1.1.1`), Google Public DNS (`8.8.8.8`), IBM Quad101.
- **Untuk Perlindungan Malware & Phishing**:
  - Quad9 Secure (`9.9.9.9`), Comodo Secure, Yandex Safe.
- **Untuk Blokir Iklan & Pelacak**:
  - AdGuard DNS, NextDNS (kustom).
- **Untuk Kontrol Parental & Blokir Konten Dewasa**:
  - Cloudflare Family, OpenDNS Family, CleanBrowsing.
- **Untuk Lingkungan Bisnis (Enterprise DNS)**:
  - UltraDNS, IBM Quad101, OpenDNS.

DNS - DNSSEC

DNSSEC (Domain Name System Security Extensions) adalah seperangkat ekstensi keamanan untuk **DNS (Domain Name System)** yang dirancang untuk melindungi pengguna dari manipulasi data DNS, seperti **DNS spoofing** atau **cache poisoning**. DNSSEC memastikan bahwa informasi yang dikirim melalui DNS berasal dari sumber yang tepercaya dan tidak diubah selama proses transmisi.

Fungsi Utama DNSSEC:

1. **Otentikasi Sumber Data**: Memastikan bahwa data DNS berasal dari server yang benar (asli).
2. **Integritas Data**: Menjamin bahwa data DNS tidak diubah atau dimanipulasi dalam perjalanan.
3. **Perlindungan dari Serangan**: Melindungi dari serangan seperti *DNS spoofing* atau *cache poisoning*.

Cara Kerja DNSSEC:

1. **Tanda Tangan Digital (Digital Signature)**:
   - Zona DNS yang diaktifkan DNSSEC akan menandatangani setiap respons menggunakan **kriptografi kunci publik**.
   - Setiap rekam DNS (seperti A, AAAA, MX) memiliki tanda tangan digital yang diverifikasi oleh resolver DNS.
2. **Verifikasi Kunci (Chain of Trust)**:
   - Dimulai dari **root zone** DNS, setiap lapisan zona DNS memverifikasi kunci publik zona di bawahnya.
   - Ini membentuk **rantai kepercayaan** (chain of trust) dari root hingga domain yang diakses.

Rekaman DNS Khusus di DNSSEC:

- **RRSIG**: Menyimpan tanda tangan digital.
- **DNSKEY**: Menyimpan kunci publik.
- **DS (Delegation Signer)**: Menghubungkan zona ke induknya.
- **NSEC/NSEC3**: Mencegah pencacahan zona dan menunjukkan catatan yang tidak ada.

Keuntungan DNSSEC:

- Perlindungan dari manipulasi data DNS.
- Meningkatkan kepercayaan dan keamanan di internet.
- Mencegah pengguna diarahkan ke situs palsu atau berbahaya.

⚠ **Kelemahan DNSSEC:**

- Kompleksitas dalam implementasi dan pengelolaan.
- Memerlukan dukungan dari seluruh rantai DNS (termasuk registrar dan resolver).
- Penambahan overhead karena verifikasi tanda tangan.

DNS - Config DNSSEC

A. Cara Mengatur DNSSEC pada Domain

Langkah-langkah mengatur DNSSEC bervariasi tergantung pada registrar (penyedia domain) dan penyedia DNS, tetapi secara umum mengikuti proses berikut:

1️⃣ **Pastikan Penyedia DNS dan Registrar Mendukung DNSSEC**

- Cek apakah registrar domain Anda mendukung DNSSEC.
- Pastikan layanan DNS (misalnya Cloudflare, Google Domains, AWS Route 53) memiliki fitur DNSSEC.

2️⃣ **Aktifkan DNSSEC di Penyedia DNS**

- Masuk ke panel kontrol penyedia DNS.
- Cari opsi **DNSSEC** dan aktifkan.
- Sistem akan menghasilkan:
  - **DNSKEY** (Kunci Publik)
  - **DS Record** (Delegation Signer Record)

3️⃣ **Tambahkan DS Record ke Registrar Domain**

- Salin **DS Record** dari penyedia DNS.
- Buka dashboard registrar (misalnya GoDaddy, Namecheap, Cloudflare).
- Temukan opsi **DNSSEC Management** atau **Advanced DNS Settings**.
- Masukkan informasi DS Record:
  - **Key Tag**: Identifikasi kunci DNSKEY.
  - **Algorithm**: Algoritma kriptografi (misal: RSA/SHA-256).
  - **Digest Type**: Metode hash (misal: SHA-256).
  - **Digest**: Hasil hash dari DNSKEY.

4️⃣ **Verifikasi Konfigurasi**

- Setelah beberapa menit hingga beberapa jam (tergantung propagasi DNS), DNSSEC akan aktif.
- Pastikan konfigurasi benar sebelum melanjutkan ke pengujian.

DNS - Testing DNSSEC

Ada beberapa Tools online dan perintah yang dapat digunakan untuk memverifikasi DNSSEC :

---

1. Menggunakan Tools Online

1. **DNSViz** – Analisis mendalam tentang status DNSSEC.
2. **Verisign DNSSEC Debugger** – Mengecek dan menganalisis pengaturan DNSSEC.
3. **Google DNSSEC Check** – Melakukan validasi DNSSEC.

Contoh Penggunaan DNSViz:

1. Buka DNSViz.
2. Masukkan nama domain Anda (contoh: `ilusidigital.com`).
3. Klik **Go** untuk memulai analisis.
4. Periksa apakah terdapat rantai kepercayaan (Chain of Trust) dari root ke domain Anda.

---

2. Menggunakan Perintah di Terminal (Linux/macOS/Windows WSL)

1. **Menggunakan `dig` (Domain Information Groper)** :

   - Periksa tanda tangan DNSSEC:

```
dig ilusidigital.com +dnssec
```

   - Cek DS Record di root zone:

```
dig ilusidigital.com DS +short
```

   Jika DNSSEC aktif, Anda akan melihat output berupa record RRSIG (tanda tangan digital).

---

3. Menggunakan `nslookup` di Windows

- Jalankan perintah:

```
nslookup -type=ds ilusidigital.com
```

Jika berhasil, akan muncul informasi DS Record.

Contoh Output yang Valid

```
ilusidigital.com. 3600 IN RRSIG A 8 2 3600 (Signature Info)
```

- **DS Record** dan **RRSIG** menunjukkan DNSSEC aktif.
- Jika tidak ada output tersebut, berarti DNSSEC belum diaktifkan.

Kesimpulan:

- **Mengatur DNSSEC** memerlukan sinkronisasi antara **penyedia DNS** dan **registrar domain**.
- **Uji DNSSEC** menggunakan alat seperti **DNSViz** atau perintah **dig** untuk memverifikasi keberhasilan konfigurasi.