PANDUAN KONFIGURASI

DOMAIN NAME SYTEM (DNS)

GOV-CSIRT (Government Computer Security Insident Response Team)

Pusat Monitoring dan Penanganan Insiden Keamanan Informasi Instansi Pemerintah

Direktorat Kemanan Informasi

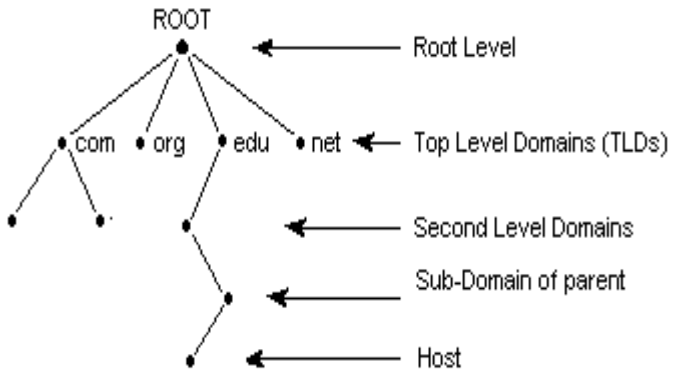
Kementerian Komunikasi dan Informatika Republik Indonesia

Overview Domain Name System

Saat ini internet merupakan jaringan komputasiterbesar di dunia.Dari perspektifpengguna, setiapnode atau sumber dayadi jaringan inidiidentifikasi dengannama yang unik: nama domain.Beberapa contohsumber daya Internetadalah:

- Web server-untuk mengakses situs Web
- Mail server-untuk menyampaikan pesan e-mail

DNS server merupakan server yang digunakan untuk me-resolve nama-nama sistem ke dalam IP address atau sebaliknya (reverse lookup). Agar fasilitas DNS server tersedia di dalam jaringan, diperlukan sebuah nameserver.DNS merupakan sebuah struktur hierarki yang digunakan untuk mengelola nama domain. Struktur yang paling atas ditandai dengan sebuah titik. Contoh dari domain puncak antara lain**.com, .edu,.gov** dan lain-lain. Nama perusahaan, organisasi biasanya merupakan domain level kedua. Supaya dapat mengakses sebuah host yang menjadi anggota dari sebuah domain, anda dapat menggunakan FQDN (*Fully Qualified Domain Name*). Dengan menggunakan FQDN DNS akan memetakan sebuah nama host ke sebuah alamat IP tertentu.



Gambar 1. Hirarki DNS

Terminologi

Terdapat beberapa istilah dan konsep yang akan kita perlukan ketika mengelola server DNS. Beberapa diantaranya adalah :

- DNS server merupakan sebuah komputer yang menyediakan service nama domain. Server DNS ini dapat berupa sebuah Primary DNS server merupakan pemilik dari zone yang didefinisikan dalam database. Server DNS memiliki otoritas untuk membuat perubahan terhadap zone yang ia miliki. Server-server DNS Secondary menerima salinan zone yang bersifat read only melalui mekanisme zone transfer. Secondary DNS Server dapat meresolusi query berdasarkan informasi salinan zone yang bersifat read-only

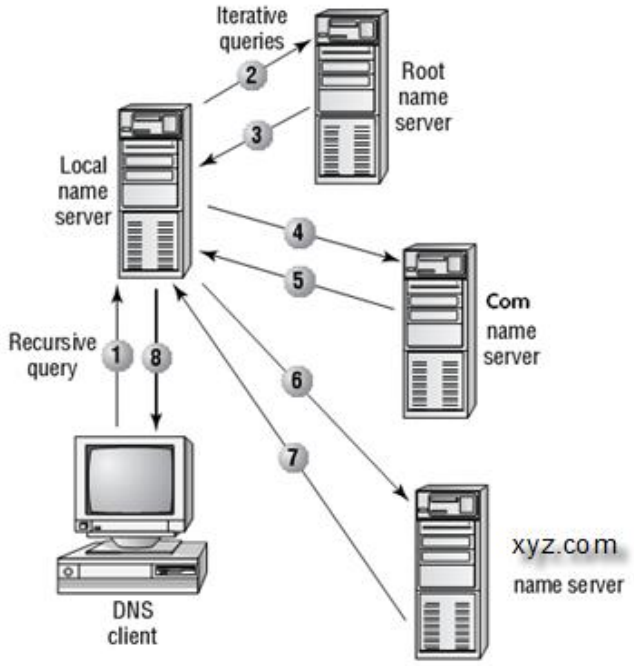
tetapi tidak dapat membuat perubahan atau update. Sebuah server DNS dapat berisi beberapa zone primer dan secondary.

- DNS Client, setiap mesin yang melakukan query ke server DNS. Hostname client dapat diregister ke dalam database DNS. Cllient-client memberikan DNS request melalui proses yang disebut resolver.
- Resolver, merupakan sebuah program klien yang berjalan di komputer pengguna, yang akan melakukan request ke DNS Recursive. Resolver memberikan query ke server DNS. Ketika sebuah resolver menerima informasi dari DNS server, ia menyimpan informasi tersebut (ke dalam cache) secara lokal, agar dapat dimanfaatkan kembali ketika ada permintaan yang sama. Ketika server DNS tidak dapat menjawab permintaan, ia akan mereply resolver dengan memberikan informasi server DNS yang lain.
- Query, terdapat dua jenis query yang dapat dibuat oleh server DNS, yakni:
    - ***Forward lookup query***, permintaan untuk memetakan sebuah FQDN dengan sebuah alamat IP
    - ***Reverse lookup query***, permintaan untuk memetakan sebuah alamat IP dengan sebuah FQDN.
- Root Server, ketika sebuah server DNS memproses sebuah query recursive dan query tidak dapat di resolusi dari file lokal zone, query harus dieskalasi ke server DNS root. Server root bertanggungjawab untuk menghasilkan sebuah jawaban untuk domain tertentu atau mengarahkan ke server lain yang dapat menyediakan jawaban yang sah. Kita juga dapat mengkonfigurasi dns kita berisi root agar ketika ada permintaan, DNS tidak akan mengarahkan ke server DNS yang lain.
- DNS Zone, server DNS bekerjasama untuk meresolusi nama secara hirarki. Jika mereka telah mempunyai informasi tentang sebuah nama, mereka akan menyederhanakan untuk memenuhi permintaan client. DNS zone merupakan bagian dari DNS namespace yang terdapat pada server DNS tertentu. Untuk menjamin mekanisme penamaan secara akurat dalam lingkungan yang terdistribusi, sebuah server DNS harus dirancang sebagai master database untuk serangkaian alamat tertentu.
- Dynamic DNS, dirancang untuk mengatasi masalah berkaitan dengan alamat dari client yang bersifat dinamis. DDNS mengijinkan client DNS untuk mengupdate informasi yang terdapat di dalam file database DNS. Sebagai contoh, sebuah DHCP server windows 2003 dapat secara otomatis memberitahukan ke server DDNS tentang alamat IP dipasang di sebuah komputer.
- Recursive DNS Server, mesin yang akan melakukan pencarian atas permintaan ”resolver” dan mesin yang akan memberikan jawaban atas permintaan tersebut.
- Authoritative DNS Server, Adalah mesin yang bertanggung jawab atas sebuah domain, dan memberikan jawaban terhadap recursor.

Cara Kerja DNS

Cara Kerja DNS dalam memecahkan masalah penamaan dan pengalamatan IP kita diuraikan sebagai berikut :

- *Client* DNS melakukan *query* (permintaan) ke *server* DNS yang sebelumnya telah dikonfigurasi untuk meresolusi nama FQDN.
- Jika *server* DNS dapat meresolusi permintaan tersebut, *server* DNS akan merespon permintaan dari *client*. Hal ini dikenal dengan istilah *iterative query*.
- Tetapi jika *server* DNS tidak dapat meresolusi permintaan tersebut, *server* DNS akan menghubungi *server* DNS yang lain, agar dapat merespon atau menjawab permintaan dari *client* DNS. Proses tersebut dikenal dengan istilah *recursive query*.



Gambar 2.Query DNS

Record-Record DNS

Resource Record merupakan record yang terdapat dalam database DNS untuk menerjemahkan IP Address ke nama dan dari Nama ke IP Address.Ada beberapa resource Record :

1. Record A : berisi nama host dan IP Address, menunjukkan alamat Ipv4. Nama owner akan ekuivalen dengan IP address yang didefinisikan setelah record A.

2. Record SOA (Start of Authority): siapa yang bertanggung jawab atas suatu zone.

   SOA MNAME ➔ SOA: Start Of Authority*SOA MNAME*> adalah field yang menunjukkan master server pada puncak/root dari zona authority. Hanya diperbolehkan terdapat satu master server tiap zona authority. Contohnya domain xyz.com memiliki SOA MNAME ns1.xyz.com

   SOA Serial Number SOA Serial Number adalah field yang menunjukkan serial number dari DNS server.Format yang paling populer dalam penamaan serial number ini adalah yyyymmddss dengan yyyy adalah tahun, mm adalah bulan, dd adalah tanggal, dan ss adalah jumlah perubahan yang dilakukan pada hari itu.Nilai dari field ini harus diubah ketika terjadi perubahan pada zone file.

   SOA REFRESH ➔ SOA REFRESH adalah field yang menunjukkan waktu slave server akan merefresh zona dari master server.

   SOA RETRY➔ SOA RETRY adalah field yang menunjukkan berapa lama waktu jeda antara percobaan slave server mengkontak master server jika kontak pertama mengalami kegagalan ketika slave master me-refresh cache dari master server.

   SOA EXPIRE➔ SOA EXPIRE adalah field yang menunjukkan berapa lama zona-data masih authoritative. Field ini hanya berlaku untuk slave atau secondary server. Ketika nilai ini telah expired, maka slave master akan mengontak master server untuk membaca SOA record pada zona dan merequest AXFR/IFXR jika serial number berubah. Jika slave gagal mengontak master, maka slave akan terus mencoba mengontak master dan masih melayani query hingga waktu SOA EXPIRE habis. Setelah itu slave akan berhenti melayani query hingga kontak ke master server berhasil. RFC 1912 merekomendasikan 1209600 hingga 2419200 (2-4 minggu).

   SOA MINIMUM TTL➔SOA MINIMUM TTL adalah nilai default TTL (Time To Live) untuk semua record pada zone file. Field ini dalam satuan detik.
3. RecordNS (Name Server): name server yang bertanggung jawab atas suatu zone
4. RecordCNAME (Canonical Name) : nama alias untuk suatu host, dan sebuah record yang menjelaskan primary name untuk owner. Nama ownernya disebutkan dalam alias.
5. Record MX(MailExchanger). SebuahRRjenis inimenyediakannama domain mail server

Lingkungan DNS

Sebelum tujuan keamanan dapat ditentukan, blok bangunan dari DNS perlu ditetapkan. DNS meliputi berikut ini:

- Platform (perangkat keras dan sistem operasi) di mana nameserver dan resolver berada
- Perangkat lunak nameserver dan resolver

  Dua komponen software utama dari DNS adalah name server dan resolver. Fungsi utama dari name server adalah untuk database host yang berisi informasi nama domain dan untuk memberikan respon terhadap permintaan resolusi nama. Fungsi utama dari perangkat lunak resolver adalah untuk merumuskan permintaan resolusi nama. Data utama dari DNS adalah file zone (file konfigurasi DNS).

- Transaksi DNS berupa :
  - Query/Respon DNS
  - Zone Transfer
  - Dynamic update
  - DNS Notify

- Database DNS (zona file)

  Zona fileberisi informasi tentangberbagai sumber dayadi zonaitu.Informasi tentangsetiap sumber dayadiwakilidalam catatanyang disebutResource Record(RR). Karenazonamungkin berisibeberapa domaindanbeberapa jenissumber daya dalamsetiap domain,format masing-masingRRberisikolom untukmembuat identifikasiini.Secara khusus, RR terdiri dari:
  - Owner name : nama domain ataunama sumber daya
  - TTL: Time to Live
  - Kelas:saat inihanya satu kelas, IN (Internetyang menunjukkan)
  - RRType: jenis sumber daya
  - RData: informasi tentangsumber daya(tergantung pada RRType)

- Konfigurasi file padanameserver dan resolver.

  Ada duajenis name server utama :Authoritative DNS server dan nama servercaching.Jika name servermerupakan sebuah sumberotoritatif untukRRpada zonatertentu, hal itu

disebut Authoritative DNS server. Sebuah serverotoritatifsebuah zonamenyediakan respon terhadappermintaan resolusi namauntuk sumber dayazona tersebut,menggunakanRR yang terdapat di dalam file zone itu sendiri.

Terdapat dua jenis server otoritatif : master (primary) dan slave (secondary).
Jenis server otoritatif slave berfungsi untuk cadangan dari server master, dengan menyediakan mekanisme fault tolerance. Sebuah server master berisi file-file zone yang dibuat dan diubah secara manual oleh administrator. Terkadang sebuah server master mengijinkan file zone di update secara dinamis oleh client DNS yang diberi hak. Sebuah server yang dikonfigurasi dengan fitur tersebut biasanya disebut primary master name server.

Sebuah server slave juga berisi informasi otoritatif dari sebuah zone, tetapi file zone ini merupakan replikasi dari server master yang berhubungan. Replikasi merupakan mekanisme yang mengijinkan sebuah transaksi yang disebut zone transfer yakni sebuah mekanisme yang mentransfer semua RR file zone dari sebuah server ke server slave. Dikarenakan sebuah permintaan resolusi nama adalah untuk sebuah RR tertentu, sebuah zone transfer dikategorikan sebagai sebuah mekanisme permintaan dengan kode AXFR, yang berarti semua RR yang terdapat pada sebuah zone diminta.

Ketika isi dari sebuah file zone yang terdapat di server master diubah, diserver-server slave menerima pemberitahuan terhadap adanya perubahan tersebut melalui sebuah transaksi yang disebut DNS NOTIFY. Ketika sebuah server slave menerima permintaan ini, slave akan menginisiasi sebuah permintaan zone transfer ke server master.

Sebuah server caching (disebut juga server resolving/recursive) menyediakan respon melalui serangkaian permintaan ke server otoritatif lainnya di dalam hierarki domain yang ditemukan dalam proses permintaan resolusi nama atau dari sebuah respon cache yang telah dibangun dengan menggunakan permintaan sebelumnya.

Sebuah servercachingumumnyaadalah server lokaldi organisasiyang melakukan fungsiresolusi namaatas namaklien-klien yang terdapat dalam organisasi. Fungsiresolusi namadilakukanoleh servercachingsebagai respon dari permintaanresolver. Prosespencarianyang melibatkan resolusi namadapat melibatkan pencarian padacache itu sendiri, permintaan dilakukan secara rekursif pada berbagai serverotoritatifataupermintaan secara iteratif,atau kombinasi darimetode ini.

Server khusus dapat dikonfigurasi sebagai server rekursif dan otoritatif.Dalam konfigurasi ini, server menyediakan informasi otoritatif terhadap permintaan yang berhubungan dengan zone otoritatif ketika server melakukan fungsi merespon terhadap permintaan ke zone lainnya.Setiapserver yang mendukungqueryrekursiflebihrentan terhadap serangandariserveryang tidak mendukungquerytersebut. Akibatnya, informasi otoritatifdapat dikompromikan. Oleh karena itu,bukan praktikkeamanan yang baik untukmengkonfigurasi serveruntuk melakukankedua fungsiotoritatif danrekursif.

Software seperti Web browser dan e-mail client yang membutuhkan akses ke sumber daya internet menggunakan klien DNS, yang disebut resolver klien atau menggunakan resolver. The resolver merumuskan permintaan resolusi nama untuk sumber daya dicari oleh perangkat lunak mengirimkannya ke server (resolving) caching nama di organisasi. Stub resolver umumnya dikonfigurasi dengan dua atau beberapa server untuk menyediakan fitur fault tolerant. Sebuah caching (resolving) nama server yang menerima permintaan dari resolver juga merumuskan permintaan untuk mengirim mereka ke server nama otoritatif (jika tidak mampu merespon permintaan dari cache).

Ancaman Terhadap Lingkungan Hosting DNS

Lingkungan hosting DNS terdiri dari unsur-unsur berikut:
• Platform host (sistem operasi, sistem file)
• Perangkat lunak DNS (nama server, resolver)
•Data DNS (file zona, file konfigurasi)

Ancaman terhadap platform Host

Ancaman terhadap platform host DNS tidak berbeda dengan ancaman yang dihadapi semua host di internet. Ancaman bersifat umum dan dampaknya adalah sebagai berikut:

- Ancaman terhadap sistem operasi, perangkat lunak sistem lainnya atau perangkat lunak aplikasi lain pada host DNS bisa rentan terhadap serangan seperti **buffer overflows**, sehingga **meniadakan layanan resolusi nama**.
- Ancaman terhadap stack TCP / IP pada host DNS dapat dimanfaatkan untuk melakukan serangan **packet flooding** (seperti SYNC dan smurf), yang mengakibatkan gangguan komunikasi .Lapisan aplikasi merupakan bagian dari serangan dengan mengirim sejumlah besar permintaan DNS palsu untuk membanjiri server DNS.
- Ancaman dari insideryang memiliki akses ke jaringan area lokal (LAN) di mana host DNS berada bisa mengirimkan serangan **Address Resolution Protocol (ARP) spoofing** yang mengganggu aliran pesan DNS.
- Ancaman terhadap file-file konfigurasiplatform (misalnya, resolv.conf dan host.conf di platform Unix), file data (file zona) dan file yang berisi kunci-kunci kriptografi dapat rusak oleh **virus dan worm** atau dimanfaatkan untuk melakukan perubahan secara tidak sah karena tidak memadainya perlindungan terhadap file, sehingga menimbulkan kerusakan jalur komunikasi antar host DNS.
- Ancaman dari sebuah host pada LAN yang sama, sebagai klien DNS mungkin dapat **mencegat dan/atau mengubah respon** yang dikirim olehserver DNS. Hal ini akan memungkinkan penyerang untuk mengarahkan klien menuju ke situs yang berbeda.

Ancaman-Ancaman pada Perangkat Lunak DNS

Ancaman terhadap perangkat lunak DNS itu sendiri dapat memiliki dampak keamanan serius. Masalah perangkat lunak yang paling umum dan dampak dari ancaman terhadap sistem adalah sebagai berikut:

- Perangkat lunak DNS yang digunakan dapat memiliki kerentanan seperti **buffer overflows** yang mengakibatkan peniadaan layanan.
- Perangkat lunak DNS **tidak menyediakan kemampuan akses kontrol** yang memadai untuk file konfigurasi (misalnya named.conf), file data (misalnya, file zona) dan file-

fileyang berisi kunci tanda tangan (misalnya, TSIG, DNSKEY) untuk mencegah file diakses secara tidak sah.

Ancaman Terhadap Isi Data DNS

Data DNS terdiri dari dua jenis: file-file zone dan file-file konfigurasi. Isi dari kedua jenis data DNS tersebut memiliki konsekuensi keamanan. Semua opsi penerapan keamanan yang dibahas dalam dokumen ini berhubungan dengan isi file konfigurasi.

Berbagai jenis isi yang tidak diinginkan dalam file zona memiliki potensi ancaman sebagai berikut:

- Lumpuhnya mekanisme Delegasi :Masalah ini terjadi ketika FQDN dan/atau alamat IP dari server yang terdapat di zona anak tetapi zona induk belum memperbarui informasi delegasi. Dalam situasi ini, zona anak menjadi tidak terjangkau.
- Zone Drift dan Zona Thrash: Jika nilai pada fieldRefresh, dan Retry yang terdapat dalam SOA RR dari server utama ditetapkan terlalu tinggi dan file zone yang sering berubah, dapat menimbulkan ketidakcocokan data antara server primer dan sekunder, masalah ini disebut zone drift.
- Jika nilai pada fieldRefresh dan Retry padaSOA RR ditetapkan terlalu rendah, server sekunder akan sering melakukan transfer zona. Masalah ini disebut zona thrash, hal itu menghasilkan beban kerja lebih diantara kedua server primer dan sekunder. Data yang salah atau beban kerja yang meningkat dapat menyebabkan penolakan layanan.
- Ancaman dengan memanfaatkanInformasi yang dimiliki Target, RRS seperti HINFO dan TXT menyediakan informasi tentang nama dan versi perangkat lunak (misalnya, untuk sumber daya seperti server web dan server mail) yang akan memungkinkan penyerang untuk mengeksploitasi kerentanan dengan mengetahui versi perangkat lunak dan melakukan serangan terhadap sumber daya tersebut.

Pengamanan Terhadap Lingkungan DNS

Pengamanan Platform Host DNS

Berdasarkan pada ancaman-ancaman yang muncul terhadap platform host DNS, pengamanan terhadap platform host DNS dapat dilakukan dengan pendekatan:

- Menjalankan sistem operasi yang aman
- Mengamankan konfigurasi sistem operasi

Platform server DNS seharus ditempatkan pada sistem operasi yang aman. Kebanyakan instalasi DNS dilakukan pada sistem operasi Unix dan Windows. Berikut ini upaya terhadap pengamanan platform server DNS yang perlu dipastikan :

- Patch sistem operasi yang terbaru sudah terinstall
- Secara khusus (idealnya), host yang menjalankan perangkat lunak server DNS tidak perlu menyediakan layanan lain dan karena itu harus dikonfigurasi untuk menanggapi lalu lintas DNS saja. Dengan kata lain, pesan masuk hanya diperbolehkan untuk host ini harus 53/udp dan 53/tcp.

Pengamanan Perangkat Lunak DNS

Pengamanan terhadap perangkat lunak DNS agar terhindar dari ancaman-ancaman yang muncul terhadap perangkat lunak DNS dapat dilakukan dengan melalui pendekatanberikut :

- Mengunakan software DNS dengan versi terakhir atau versi sebelumnya dengan patch yang sesuai.
- Menonaktifkan fitur tanggapan terhadap versi
- Menjalankan perangkat lunak dengan hak akses terbatas
- Mengisolasi/Melindungi software server DNS
- Menetapkan sebuah server dedicated untuk setiap fungsi
- Menghapus host yng tidak diperlukan pada software server nama
- Membatasi informasi resource IT melalui dua file zone berbeda di dalam server fisik yang sama atau melalui server nama terpisah untuk dua kelas klien yang berbeda.

Perlindungan terhadap perangkat lunak DNS terdiri dari :

- Mengunakan software DNS dengan versi terakhir atau versi sebelumnya dengan patch yang sesuai.
    - Ketika menginstal versi upgrade dari perangkat lunak server, administrator harus membuatperubahan yang diperlukan untuk parameter konfigurasi dengan memanfaatkan fitur keamanan baru.
    - Ketikamenggunakan versi terbaru atau versi sebelumnya, administrator harus menyadari kerentanan, eksploitasi, perbaikan keamanan, dan patch untuk versi yang beroperasi di organisasi. Alamat http://www.isc.org/products/BIND/bind-security.html dapat dijadikan referensi untuk mengetahui kelemahan perangkat lunak BIND (perangkat lunak DNS), sebaiknya dipantau secara periodic.

- Menonaktifkan fitur tanggapan terhadap versi
    - Untuk mencegahinformasi tentangversisoftware yang digunakan server,DNSharus dikonfigurasi untukmenolakpermintaan untukinformasiversi.

- Menjalankan perangkat lunak dengan hak akses yang terbatas
  Jika perangkat lunakserver dijalankan dengan menggunakan account priviledge (misalnya,root disistem Unix atau administrator di sistem windows), dapat memilikikonsekuensi bencanaterhadap sumber dayasistem.Secara khusus, seorang hacker yang membobolperangkat lunakmemperolehakses tidak terbatasdan karena itudapatberpotensi mengeksekusi perintah atau memodifikasi atau menghapus file. Oleh karena itu, perlu untuk menjalankan perangkat lunak server DNS sebagai pengguna nonprivileged dengan akses terbatas.

- Mengisolasi Perangkat Lunak Server
  Jika perangkat lunak DNS (misalnya, BIND) dijalankan pada OS aman, kerentanan program perangkat lunak lain pada platform tersebut dapat melanggar keamanan perangkat lunak DNS. Oleh karena itu, dianjurkan bahwa platform di mana perangkat lunak DNS berjalan tidak berisi program-program selain yang diperlukan untuk mendukung OS dan jaringan. Jika hal ini tidak mungkin karena keterbatasan sumber daya, perawatan harus dilakukan untuk memastikan untuk membatasi jumlah service yang berjalan pada platform yang sama.

- Non aktifkan fitur Recursive pada Authoritative Server DNS
  Sebuah Authorative server DNS hanya dimaksudkan untuk menyediakan resolusi nama untuk zona yang memiliki informasi otoritatif. Oleh karena itu, kebijakan keamanan yang diterapkan adalah menonaktifkan fitur rekursi pada jenis server ini. Menonaktifkan rekursi mencegah Authorative server DNS dari mengirim permintaan atas nama server lain dan membangun cache menggunakan tanggapan. Menonaktifkan fungsi ini

menghilangkan ancaman keracunan cache pada otoritatif melayani dan mencegah penggunaannya sebagai reflektor untuk serangan DDoS.

- Menghapus Perangkat Lunak DNS dari host yang bukan berperan sebagai DNS
  Perangkat lunakDNStidak bolehberjalan atauterdapat padahost yangtidak ditujukan sebagaiserver DNS.Beberapa sistem operasi secara default telah menginstallkan perangkat lunak DNS.Oleh karena itu, saat melakukaninventarisasiperangkat lunak padaworkstation dan serverdari perusahaansebagai bagian dariaudit keamanan, perlu untuk mencariinstalasiBIND danmenghapusnya darihost yang tidak berfungsisebagai serverDNS.

- Pemasangan Authorotative server DNS berbasis Jaringan dan Lokasi Geografik
  Authorative server DNS untuk suatu organisasi seharusnya disebar berbasis pada jaringan dan lokasi geografis.Penyebaran berbasis jaringan berbasis dilakukan dengan memastikan bahwa semua server DNS tidak di belakang router, dalam sebuah subnet tunggal, atau menggunakan leased line tunggal.Penyebaran berbasis geografisdilakukan dengan memastikan bahwa tidak semua server berada di lokasi fisik yang sama.

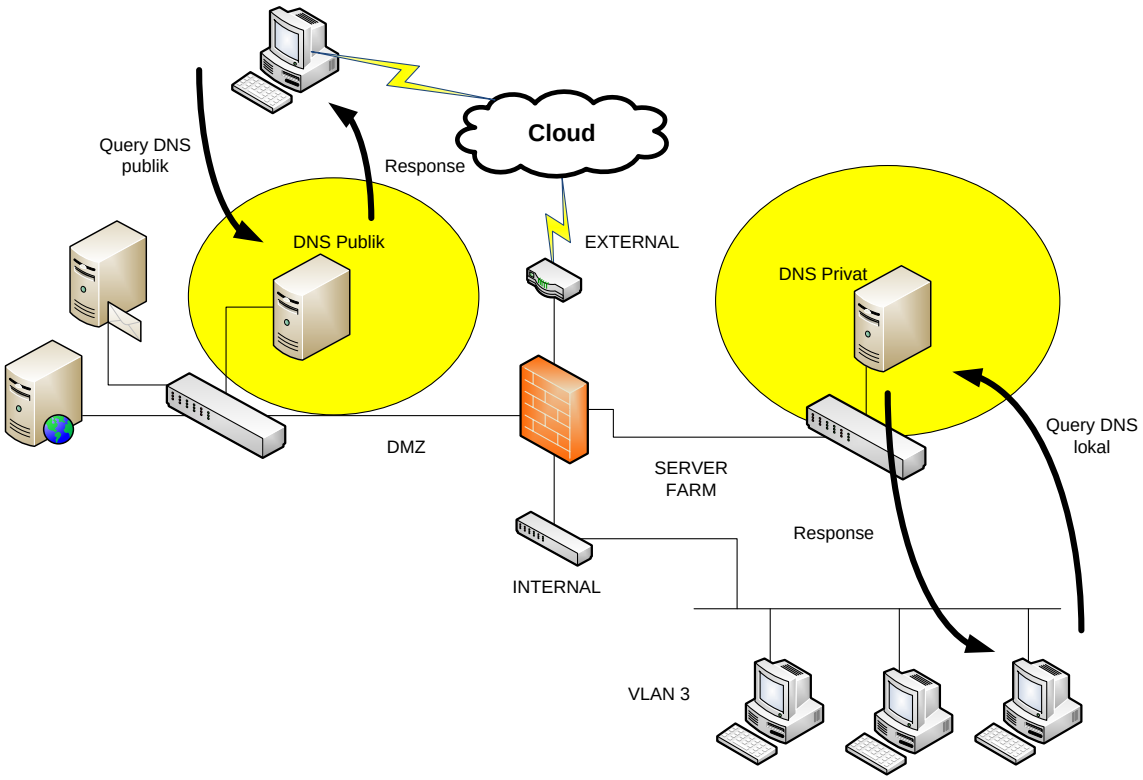
  Jika master tersembunyi digunakan, authoritative server DNS master tersembunyi hanya menerimapermintaan zone transfer dariserangkaian server secondary danmenolak semuapermintaan DNSlain.Alamat IPdari mastertersembunyitidakakan muncul dalamserverdalam databasezona.

- Membatasi informasi melalui partisi file Zone
  Server DNS otoritatif untuk suatu organisasi menerima permintaan dari klien eksternal dan internal. Dalam banyak kasus, klien-klien eksternal harus hanya menerima RR yang berhubungan untuk pelayanan publik (Web server publik, mail server, dll) klien internal harus menerima RR yang berkaitan dengan pelayanan publik serta host internal. Oleh karena itu, informasi zona yang melayani RR ini dapat dipecah menjadi file fisik yang berbeda bagi kedua jenis klien tersebut, satu untuk klien eksternal dan satu untuk klien internal.

  Split DNS memang memiliki beberapa kelemahan, diantaranya :
  Remote host mungkin tidak menggunakan server DNS resolving intenal, dan karena itu tidak mungkin dapat melihat host internal.

  - Implementasi split DNS, seharusnya memiliki minimal dua file fisik. Satu secara khusus menyediakan resolusi nama host yang ditempatkan di dalam firewall dan file ini dapat berisi serangkaian RR untuk host di luar firewall. File lain seharusnya menyediakan resolusi nama hanya untuk host terletak di luar firewall atau di DMZ.

- Membatasi Informasi melalui server terpisah untuk klien berbeda
  Teknik ini menyediakan dua server otoritatif berbeda untukmelayaniberbagai jenisklien.Yang pertama disebut server DNSeksternal,dapat terletakdalamDMZ, ini akan menjadiserverDNSbagi klieneksternal danakan menyediakan RR yangberkaitan denganhost pelayanan publik(Webserver yangmelayani halamanWeb eksternal, mailserver, dll) yang lain, yang disebut serverDNS internal, harus terletak di dalamfirewall danharus dikonfigurasisehingga merekatidak dapat dijangkau dariluardan hanya memberikanlayananpenamaansecara khusus untukklien internal.



Gambar 3.Pemisahan DNS local dan DNS publik

Pengamanan Terhadap Transaksi DNS

Perlindungan terhadap protokol DNS dalam melakukan proses transaksi dapat dilakukan melalui pendekatan berikut :

- Pembatasan terhadap entitas transaksi berbasis alamat IP
- Perlindungan transaksi melalui mekanisme otentikasi
- Perlindungan transaksi melalui Asymmetric Digital Signatures

Pembatasan terhadap entitas transaksi berbasis alamat IP

Beberapa DNS server menyediakan kemampuan akses control yang memungkinkan untuk menetapkan host yan dapat berpartisipasi dalam transaksi DNS.Host dapat diidentifikasi berdasarkan pada alamat IP dan subnet IP.

Mekanisme pembatasan transaksi ini dilakukan terhadap :

- Membatasi entitas yang dapat melakukan transaksi query/respon DNS
  Menetapkan daftar IP dan prefix IP yang dapat bertransaksi dengan server DNS.Direkomendasikan bahwa administrator membuat daftar nama dari host yang terpercaya (atau host daftar hitam) untuk setiap jenis transaksi DNS. Secara umum, peran dari kategori berikut dari host-host berikut dipertimbangkan untuk dimasukkan dalam ACL yang sesuai:
  - Host DMZ didefinisikan dalam salah satu zona
  - Semua server DNS sekunder yang diizinkan untuk melakukan transfer zona
  - Host internal yang diperbolehkan untuk melakukan query rekursif.

- Membatasi Query Rekursif
  Mematikan fiturpermintaanrekursisehingga serverDNS otoritatiftidak meracunicachedengan queryDNS lain.Sebuah serverresolverdapat dikonfigurasiuntuk menerimaqueryhanya darihost internal, untuk melindungi dariserangan denial-of-service.

- Membatasi Entitas Transaksi Zone Transfer
  DNS server yang secara periodik perlu memperbarui file zone adalah DNS server sekunder. Oleh karena itu, zone transfer hanya dibatasi pada server DNS primer ke server DNS sekunder.

- Membatasi Entitas yang melakukan update secara dinamis

Permintaan update secara dinamis umumnya berasal dari host seperti server DHCP yang memberikan alamat IP secara dinamis ke host. Setelah mereka menetapkan alamat IP untuk host baru, mereka perlu menyimpan informasi pemetaan FQDN ke alamat IP (dengan menciptakan nilai A RR) dan pemetaan alamat IP ke FQDN (dengan menciptakan RR PTR) pada server DNS otoritatif utama. Pembuatan informasi ini terjadi melalui update dinamis.

Checklist

No	Action	Check
1	Patch sistem operasi yang terbaru sudah terinstall	
2	Secara khusus (idealnya), host yang menjalankan perangkat lunak server DNS tidak perlu menyediakan layanan lain dan karena itu harus dikonfigurasi untuk menanggapi lalu lintas DNS saja. Dengan kata lain, pesan masuk hanya diperbolehkan untuk host ini harus 53/udp dan 53/tcp.	
3	Gunakan software DNS dengan versi terakhir atau versi sebelumnya dengan patch yang sesuai	
4	Nonaktifkan fitur tanggapan terhadap versi	
5	Jalankan perangkat lunak dengan hak akses yang terbatas	
6	Isolasi Perangkat Lunak Server	
7	Non aktifkan fitur Recursive pada Authoritative Server DNS	
8	Hapus Perangkat Lunak DNS dari host yang bukan berperan sebagai DNS	
9	Implementasi topologi DNS berbasis pada pengguna eksternal dan internal	
10	Batasi entitas yang dapat melakukan transaksi query/respon DNS	
11	Batasi Query Rekursif	
12	Batasi Entitas Transaksi Zone Transfer	
13	Batasi Entitas yang melakukan update secara dinamis	