BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM INTERNET VIỆT NAM

DNSSEC.vn

TÀI LIỆU

HƯỚNG DẪN TRIỂN KHAI DNSSEC TẠI CÁC DNS HOSTING PROVIDER

Quản lý phiên bản tài liệu:

Phiên bản	Ngày cập nhật	Ghi chú
1.0	10/12/2017	Biên soạn
2.0	12/11/2018	Cập nhật lần 1
3.0	18/9/2019	Cập nhật lần 2

MỤC LỤC

DANH MỤC CÁC KÝ HIỆU, CHỮ VIẾT TẮT

ccTLD	Country Code Top Level Domain
DNS	Domain Name System
DNSKEY	Domain Name System KEY
DNSSEC	Domain Name System Security Extensions
DS	Delegation Signer
EPP	Extensible Provisioning Protocol
gTLD	Generic Top-level Domain
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISP	Doanh nghiệp Internet
KSK	Key Signing Key
NĐK	Nhà đăng ký
NSEC	Next Secure
RFC	Request for Comments
RRSIG	Resource Record Signature
SRS	Shared Registry System
TLD	Top Level Domain
VNNIC	Vietnam Internet Network Information Center
ZSK	Zone Signing Key

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

MỞ ĐẦU

Hệ thống DNS đóng vai trò dẫn đường trên Internet, được coi là một hạ tầng lõi trọng yếu của hệ thống Internet toàn cầu. Do tính chất quan trọng của hệ thống DNS, đã có nhiều cuộc tấn công, khai thác lỗ hổng của hệ thống này với quy mô lớn và tinh vi với mục đích làm tê liệt hệ thống này hoặc chuyển hướng một tên miền nào đó đến một địa chỉ IP khác. Trên thế giới từ nhiều năm đã có nhiều cuộc tấn công làm thay đổi dữ liệu tên miền, chuyển hướng website được thực hiện, gây hậu quả nghiêm trọng.

Để giải quyết các nguy cơ ở trên, ngay từ năm 1990, các giải pháp khắc phục đã được nghiên cứu. Năm 1995, giải pháp DNSSEC được công bố và tới năm 2001 thì được xây dựng thành các tiêu chuẩn RFC dự thảo, và cuối cùng được IETF chính thức công bố thành tiêu chuẩn RFC vào năm 2005.

DNSSEC dựa trên nền tảng mã hoá khoá công khai (PKI) tương tự hệ thống chứng thực điện tử (CA), thực hiện ký số trên các bản ghi DNS để đảm bảo tính xác thực, toàn vẹn của cặp ánh xạ tên miền – địa chỉ IP, tất cả các thay đổi bản ghi DNS đã được ký số sẽ được phát hiện.

Kể từ khi được chuẩn hoá năm 2005, DNSSEC đã nhanh chóng được triển khai rộng rãi trên mạng Internet. Tại Việt Nam, việc triển khai áp dụng tiêu chuẩn DNSSEC cho hệ thống máy chủ tên miền (DNS) ".VN" sẽ giúp đảm bảo chính xác, tin cậy việc sử dụng, truy vấn tên miền ".VN" trên Internet thông qua việc áp dụng thống nhất tiêu chuẩn DNSSEC đối với các hệ thống DNS ".VN". Đảm bảo kết nối liên thông theo tiêu chuẩn DNSSEC giữa hệ thống DNS quốc gia ".VN" với hệ thống máy chủ tên miền gốc (DNS ROOT) và các hệ thống DNS quốc tế. Đánh dấu bước chuyển biến quan trọng trong việc phát triển hạ tầng Internet tại Việt Nam, sẵn sàng đẩy mạnh phát triển các dịch vụ thương mại điện tử, chính phủ điện tử tại Việt Nam một cách an toàn nhất.

HƯỚNG DẪN TRIỂN KHAI DNSSEC TẠI CÁC DNS HOSTING PROVIDER

1. DNS Hosting Provider:

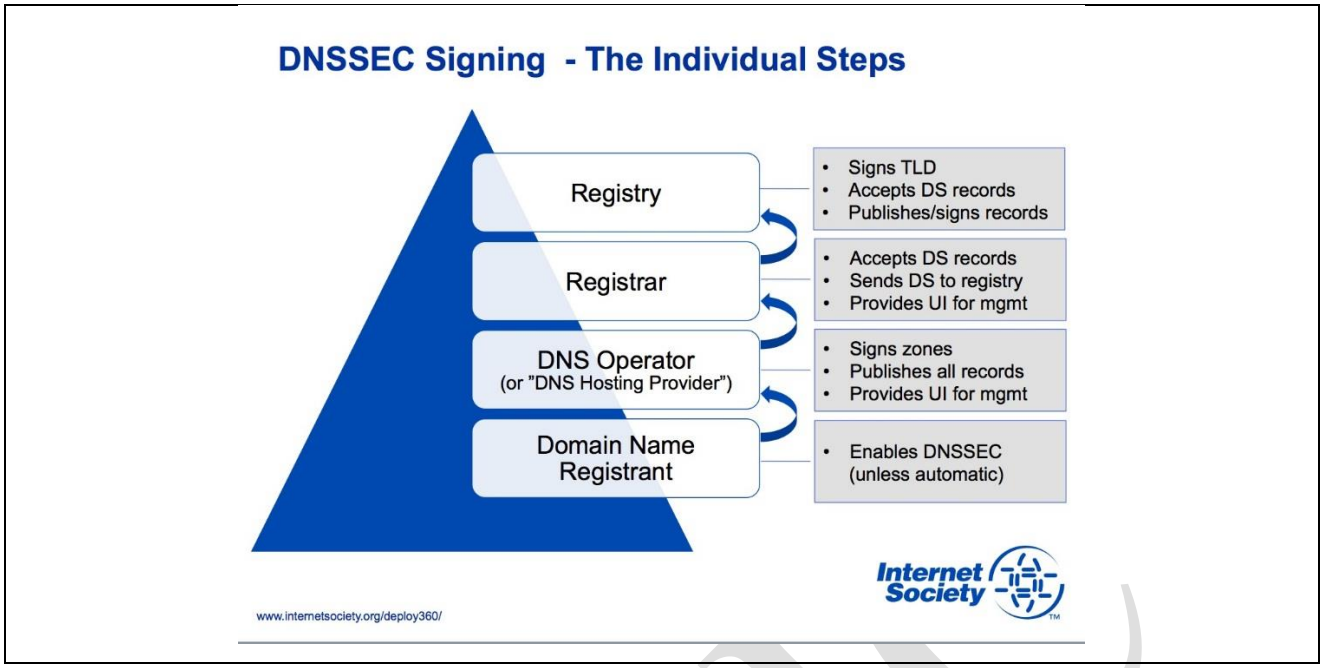
Là đơn vị cung cấp dịch vụ quản lý, lưu giữ hệ thống DNS cho các chủ thể đăng ký tên miền có nhu cầu. Trong triển khai DNSSEC, các tổ chức này phải hỗ trợ triển khai DNSEC khi khách hàng yêu cầu. Các công việc thực hiện sẽ là tạo ra các khóa (KSK, ZSK) và ký lên các zone tên miền của họ quản lý. Họ có thể cho phép xác thực nguồn gốc và toàn vẹn dữ liệu của các zone mà họ quản lý thông qua việc đăng ký bản ghi chuyển giao (DS) lên cơ quan đăng ký tên miền (Registry) thông qua các nhà đăng ký (Registrar). Trong một số trường hợp, các đơn vị này cũng là đơn vị nhà đăng ký tên miền.

2. Phân tích, đánh giá vai trò

Thông thường, sau khi một cá nhân, tổ chức thực đăng ký tên miền, sẽ phải thực hiện đăng ký chuyển giao quản lý tên miền đó về DNS Hosting.

Trong trường hợp, chủ thể tên miền muốn thực hiện triển khai ký DNSSEC cho tên miền của mình, thì quản trị DNS Hosting sẽ phải triển khai các nội dung sau:

- Tạo cặp khóa cho tên miền đăng ký DNSSEC.
- Ký DNSSEC cho tên miền đó
- Cập nhật bản ghi DS lên DNS cha. (thông thường, việc này được thực hiện thông qua các Nhà đăng ký)
- Sau đó, DNS Hosting phải thực hiện việc quản lý, duy trì các cặp khóa DNSSEC và thực hiện cập nhật các thay đổi khi cần thiết.

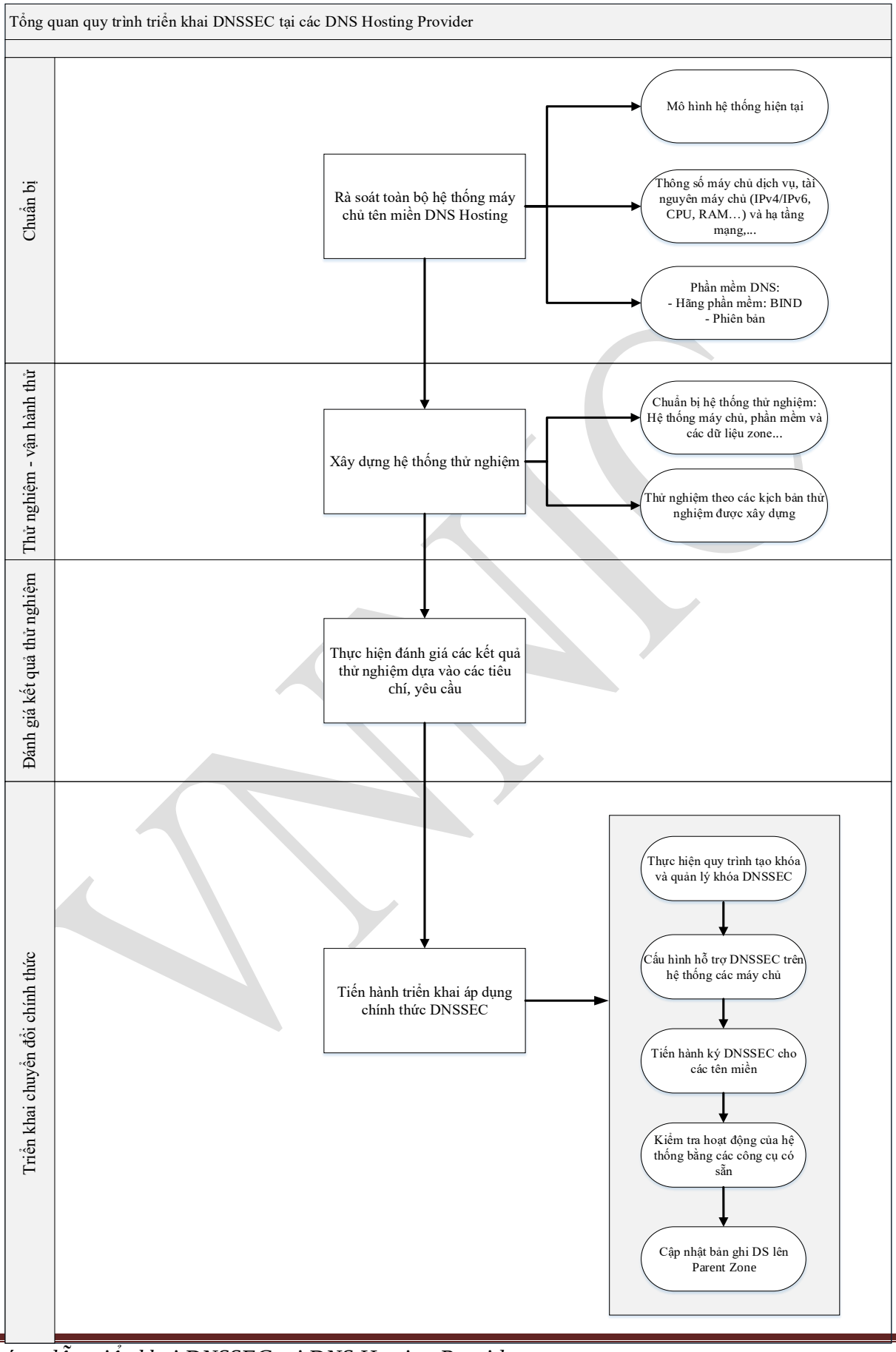


Hình 1: Mô hình mối tương quan trong hệ thống DNSSEC

Trong phạm vi tài liệu này, nhóm sẽ hướng dẫn cách thức để 1 DNS Hosting triển khai hệ thống hỗ trợ DNSSEC, còn đối với các bước thực hiện cập nhật bản ghi DS, v.v. sẽ được quy trình hóa trong các quy trình nghiệp vụ của VNNIC, Nhà đăng ký tên miền và sẽ được thông báo tới các DNS Hosting Provider theo kênh nghiệp vụ.

3. Quy trình triển khai DNSSEC

3.1. Tổng quan quy trình thực hiện


Tổng quan quy trình triển khai DNSSEC tại các DNS Hosting Provider
Chuẩn bị
Rà soát toàn bộ hệ thống máy chủ tên miền DNS Hosting
Mô hình hệ thống hiện tại
Thông số máy chủ dịch vụ, tài nguyên máy chủ (IPv4/IPv6, CPU, RAM…) và hạ tầng mạng,...
Phần mềm DNS:
- Hãng phần mềm: BIND
- Phiên bản
Thử nghiệm - vận hành thử
Xây dựng hệ thống thử nghiệm
Chuẩn bị hệ thống thử nghiệm: Hệ thống máy chủ, phần mềm và các dữ liệu zone...
Thử nghiệm theo các kịch bản thử nghiệm được xây dựng
Đánh giá kết quả thử nghiệm
Thực hiện đánh giá các kết quả thử nghiệm dựa vào các tiêu chí, yêu cầu
Triển khai chuyển đổi chính thức
Tiến hành triển khai áp dụng chính thức DNSSEC
Thực hiện quy trình tạo khóa và quản lý khóa DNSSEC
Cấu hình hỗ trợ DNSSEC trên hệ thống các máy chủ
Tiến hành ký DNSSEC cho các tên miền
Kiểm tra hoạt động của hệ thống bằng các công cụ có sẵn
Cập nhật bản ghi DS lên Parent Zone

Mô tả quy trình triển khai DNSSEC trên các DNS Hosting Provider:

- Giai đoạn 1: Các công tác chuẩn bị:

Thực hiện rà soát hiện trạng toàn bộ hệ thống về mô hình hoạt động, các thông số của hệ thống máy chủ, hạ tầng mạng và phần mềm DNS đang được sử trên hệ thống DNS của các DNS Hosting Provider.

- Giai đoạn 2: Thử nghiệm – vận hành thử:

Dựa vào kết quả rà soát mô hình hệ thống hiện tại, giai đoạn này sẽ tiến hành xây dựng nâng cấp một hệ thống triển khai thử nghiệm DNSSEC đáp ứng theo các yêu cầu trước khi triển khai và thực hiện theo các kịch bản thử nghiệm.

- Giai đoạn 3: Đánh giá kết quả thử nghiệm
- Giai đoạn 4: Tiến hành triển khai áp dụng chính thử DNSSEC:

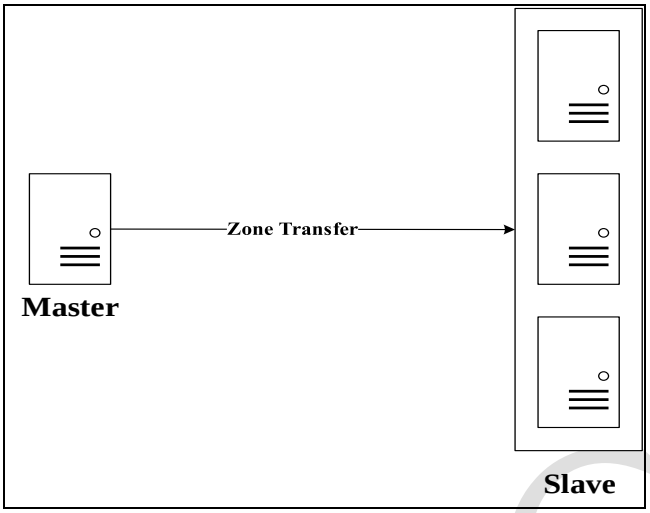
Sau khi đánh giá kết quả thử nghiệm, hệ thống thử nghiệm hoạt động tốt sẽ tiến hành triển khai áp dụng chính thức dựa theo hướng dẫn chi tiết triển khai.

3.2. Rà soát hệ thống máy chủ

Để đảm bảo việc triển khai không bị sai sót, cũng như để có thể roll back lại hệ thống cũ, thì đây là một bước quan trọng không thể thiếu; bao gồm các tiêu chí sau:

Mô hình hiện tại:

Mô hình hệ thống DNS Hosting phổ biến hiện tại của các tổ chức DNS Hosting Provider bao gồm 01 máy chủ DNS Master và nhiều máy chủ DNS Slave.



Hình 2: Mô hình hệ thống DNS Hosting phổ biến hiện nay

- Checklist các thông tin rà soát liên quan đến hệ thống máy chủ DNS Hosting:

STT	Tên máy chủ	Địa chỉ IPv4 / IPv6	Phần mềm DNS	Ghi chú
1	DNS Master		BIND 9.10	
2	DNS Slave 01			
3	DNS Slave 02			
4				

Bảng 1: Checklist rà soát thông tin hệ thống máy chủ DNS Hosting

- Các zone đang được quản lý trên hệ thống DNS Hosting:
    - Danh sách các Zone đang quản lý:

STT	Danh sách zone	Chủ thể	Ghi chú
1	zone1.vn		
2	zone2.vn		
3	labdnssec.vn		
4	….		

Bảng 2: Bảng thống kê danh sách các zone được quản lý

- Các file dữ liệu tên miền liên quan:

Đơn vị cần thực hiện backup toàn bộ hệ thống dữ liệu tên miền, việc thực hiện backup càng gần với thời điểm chuyển đổi thì càng đảm bảo thành công trong việc rollback. Ngoài ra, cần phải tiến hành kiểm thử các dữ liệu Backup, để đảm bảo dữ liệu có thể khôi phục được khi cần.

STT	Các file cần Backup	Ngày Backup	Nơi lưu bản Backup	Kết quả kiểm thử	Ghi chú
1	File cấu hình				
2	Thư mục chứa Cơ sở dữ liệu				
3	Các file liên quan.				
4	….				

Bảng 3: Danh sách các thư mục, tập tin cần được backup trước khi triển khai DNSSEC

Trong trường hợp cần thiết và điều kiện cho phép, đơn vị nên xây dựng sẵn sàng các hệ thống dự phòng.

3.3. Các yêu cầu trước khi triển khai

3.3.1. Hạ tầng vật lý:

Để đảm bảo tính an toàn của hệ thống, thông thường hệ thống DNSSEC sẽ được đặt trong một vùng riêng biệt, có quy trình giám sát nghiêm ngặt. Trong trường hợp điều kiện của đơn vị không đảm bảo, thì có thể quy hoạch các vùng dùng riêng và thực hiện quản lý thông qua các chính sách thích hợp, để đảm bảo chỉ có người có trách nhiệm mới tiếp cận được vào hệ thống.

3.3.2. Hệ thống tạo, quản lý khóa và ký DNSSEC:

Hiện nay, có rất nhiều hệ thống, công cụ hỗ trợ việc tạo, quản lý khóa và ký DNSSEC, tùy thuộc vào chính sách cũng như ngân sách của đơn vị, mà có thể chọn các giải pháp khác nhau như: Lựa chọn các thiết bị chuyên dụng, sử dụng các phần mềm mã nguồn mở, hoặc sử dụng luôn tính năng tích hợp trên phần mềm DNS của máy chủ.

3.3.3. Yêu cầu về phần mềm DNS

Hiện tại, như đã phân tích trong các tài liệu trước đây, cũng như trong các khóa đào tạo mà VNNIC đã triển khai, thì có rất nhiều phần mềm DNS đã hỗ trợ triển khai DNSSEC. Tuy nhiên, trong phạm vi này, nhóm sẽ sử dụng phần mềm BIND để làm phần mềm hướng dẫn, triển khai hệ thống DNSSEC.

Phần mềm BIND (the Berkeley Internet Name Daemon) là phần mềm DNS phổ biến nhất trên Internet, và được phát hành bởi ISC (the Internet System Consortium, http://www.isc.org).

3.3.4. Năng lực máy chủ hệ thống

Thông thường, khi triển khai DNSSEC, hệ thống sẽ phải chịu thêm tải truy vấn, cũng như việc thực hiện ký DNSSEC sẽ làm tăng CPU của hệ thống. Cũng như việc kích thước file dữ liệu tăng làm cho dung lượng chiếm dụng của ổ cứng tăng theo.

- CPU: *Tăng khoảng 1.5 lần*

Đối với máy chủ DNS dùng để ký (DNS Signer): Kích hoạt DNSSEC trên các máy chủ này đồng nghĩa với việc thực hiện quá trình ký định kỳ các zone bằng các cơ chế mã hóa chuyên sâu nên sẽ chiếm một lượng tài nguyên của máy chủ và thường xuyên dẫn đến gia tăng việc sử dụng CPU. Do vậy cần tăng các thành phần CPU, RAM cho máy chủ DNS.

Ngoài ra, nếu các DNS Hosting cho phép truy vấn đệ quy từ các Client, thì hệ thống cũng sẽ phải thực hiện các truy vấn đệ quy liên quan đến DNSSEC, do đó CPU, RAM cũng

phải tăng theo (tham khảo phần tài liệu hướng dẫn triển khai DNSSEC Caching để có đầy đủ thông tin hơn)

- Bộ nhớ hệ thống: *Tăng khoảng 3 lần.*

Quá trình ký sẽ tạo ra các tập tin dữ liệu zone (signed) có kích thước lớn hơn nhiều so với các zone khi chưa ký (unsigned) và sẽ chiếm không gian bộ nhớ lớn hơn thường gấp ba lần so với thông thường. Đặc thù của các DNS Hosting là chứa một số lượng rất lớn các bản ghi, nên việc rà soát, xem lại dung lượng ổ cứng máy chủ là một điều hết sức quan trọng đối với DNS Hosting.

3.3.5. Hạ tầng mạng

- Lưu lượng mạng tăng:

Khi triển khai áp dụng xác thực DNSSEC trên máy chủ DNS của các nhà cung cấp dịch vụ DNS Hosting, DNSSEC sẽ đính kèm chữ ký số vào gói tin phản hồi truy vấn DNS và quá trình đồng bộ dữ liệu (Zone transfer) giữa các máy chủ, điều này làm tăng kích thước của gói tin.

- Hạ tầng mạng phải đáp ứng:

Với các phản hồi truy vấn đối với DNS thông thường, kích thước gói tin không vượt quá 512 byte. Đối với DNSSEC, kích thước các gói tin có thể lớn hơn nhiều và thường xuyên vượt quá 1500 byte. Do vậy cần phải đảm bảo rằng cơ sở hạ tầng mạng là phù hợp và đáp ứng tốt.

Dưới đây là một số yêu cầu về hạ tầng mạng cần đáp ứng để có thể triển khai DNSSEC:

- DNS over TCP:

Theo truyền thống, DNS hoạt động dựa trên giao thức UDP để truyền tải các truy và trả lời. Tuy nhiên trong một số trường hợp, các đáp ứng DNS có kích thước gói tin vượt quá mức tối đa dẫn đến việc đưa giao thức TCP sử dụng là hoàn toàn có thể.

Do vậy cần phải cho phép, kiểm tra kết nối mạng qua giao thức TCP port 53 trên hệ thống hạ tầng mạng để đảm bảo rằng "DNS over TCP" được phép hoạt động.

- Kích thước gói UDP:

DNSSEC hoạt động cũng một phần dựa trên giao thức mở rộng của DNS được gọi là EDNS0. Với giao thức này sẽ làm cho DNS có thể sử dụng gói tin lớn hơn 512 byet để truyền tải đáp ứng truy vấn DNS. Nhiều phần mềm DNS (trong đó có BIND) được cấu hình quy định kích thước gói EDNS0 là 4KB, điều này có nghĩa rằng các máy chủ DNS có thể nhận được các gói tin với kích thước lên đến 4KB.

Các vấn đề như là hệ quả của việc trên:

- Một số hệ thống tường lửa (firewall) được cấu hình loại bỏ các gói tin UDP DNS có kích thước lớn hơn 512 byte vì được xem như một cuộc tấn công.
- Một số hệ thống tường lửa cũng từ chối chấp nhận các gói tin UDP phân mảnh, và đây cũng có thể được cho là dấu hiệu của tấn công.

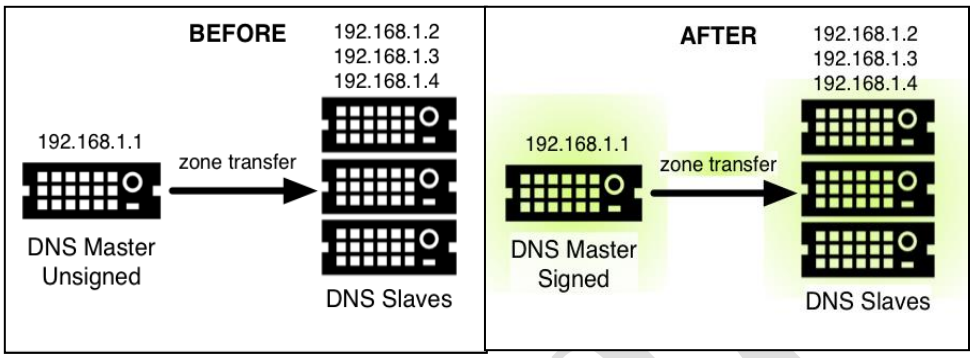
Do vậy, trong cả hai trường hợp đó, cần phải thực hiện cấu hình lại tường lửa dỡ bỏ các hạn chế, để đảm bảo hệ thống mạng có khả năng xử lý các gói tin UDP lớn (>512 byte, ≤4000 byte).

3.4. Mô hình triển khai

Dưới đây là hai mô hình triển khai DNSSEC trên hệ thống DNS Hosting Provider phổ biến:

- Mô hình Inline – Signing Box-tobox

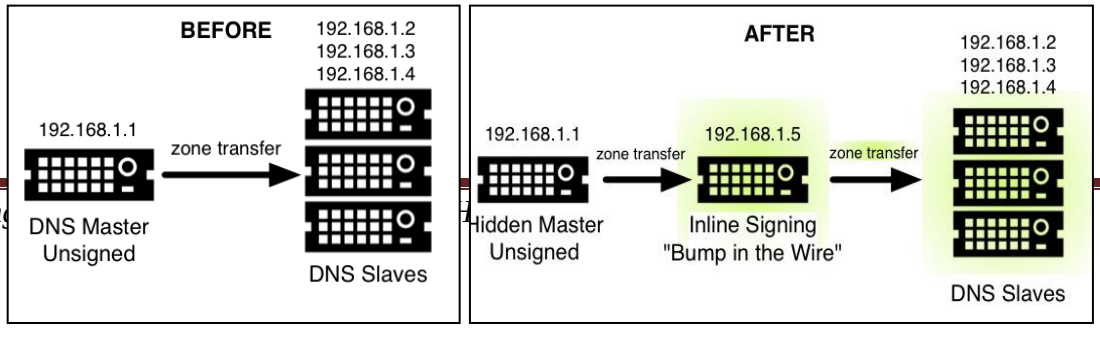
Trong mô hình này, khi triển khai DNSSEC, máy chủ DNS Master sẽ vừa là máy chủ DNS Master thông thường vừa là máy chủ DNS Signer (thực hiện chức năng ký DNSSEC). Như vậy máy chủ DNS Master sẽ đồng thời thực hiện hai chức năng, việc này sẽ gây ảnh hưởng đến tài nguyên của máy chủ và tăng mức độ rủi ro của toàn hệ thống.



Hình 3: Mô hình Inline – Signing Box-to-box

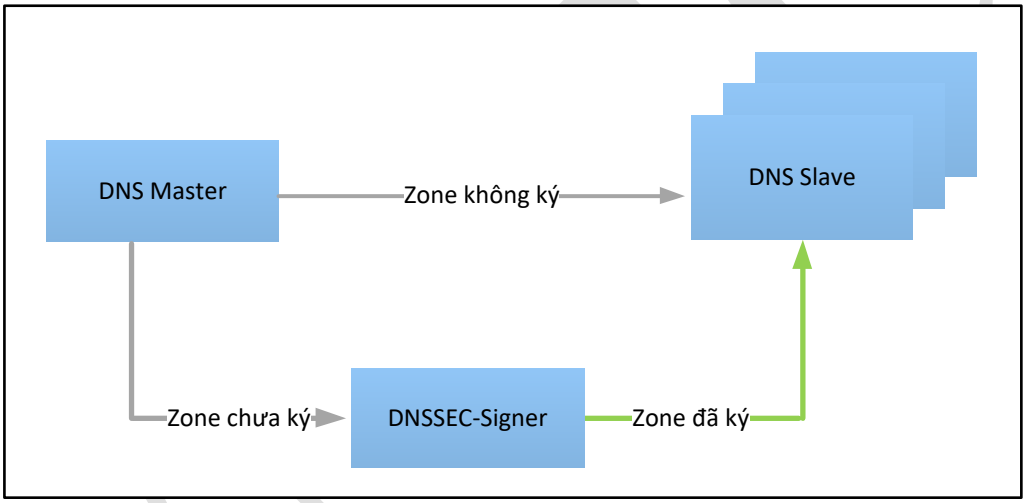
- Mô hình Inline – Signing Bump in the wire

Trong mô hình này, khi triển khai DNSSEC, sẽ triển khai thêm 01 máy chủ DNS Signer vào giữa máy chủ DNS Master (DNS Hidden) và các máy chủ DNS Slave. Máy chủ DNS Signer là slave của DNS Hidden và là master cho các máy chủ DNS Slave. Máy chủ DNS Hidden sẽ zone transfer về máy chủ DNS Signer; trên DNS Signer sẽ thực hiện chức năng ký DNSSEC và zone transfer về lại cho các máy chủ DNS Slave. Đối với mô hình này không làm ảnh hưởng đến tài nguyên của máy chủ DNS Hidden và giảm được rủi ro cho hệ thống. Khuyến nghị nên áp dụng mô hình này vào việc triển khai DNSSEC cho hệ thống DNS.



Hình 4: Mô hình Inline – Signing Bump in the wire

Tuy nhiên, do các hệ thống DNS Hosting thường đang cung cấp dịch vụ, việc ký DNSSEC không phải là ngay lập tức cho tất cả tên miền, để không làm ảnh hưởng đến các tên miền còn lại, nhóm đề xuất mô hình nguyên lý triển khai DNSSEC cho các nhà cung cấp dịch vụ DNS Hosting như sau (dựa trên mô hình *Inline – Signing Bump in the wire):*



Hình 5: Mô hình nguyên lý triển khai DNSSEC

- Mô tả hệ thống:

Hệ thống bao gồm các máy chủ DNS Master, DNS Slave và máy chủ ký DNSSEC-Signer. Theo hệ thống DNS thông thường các máy chủ DNS Master sẽ đồng bộ (zone transfer) các zone xuống DNS Slave. Khi triển khai DNSSEC, theo khuyến nghị nên triển khai thêm 01 máy chủ DNSSEC Signer dùng để thực hiện chức năng tạo khóa và ký và giữa máy chủ DNS Master và DNS Slave, do khi triển khai thực hiện chức năng tạo khóa và ký trên một máy chủ riêng biệt sẽ giúp tránh ảnh hưởng đến tài nguyên máy chủ DNS Master và toàn bộ hệ thống.

- Nguyên lý hoạt động:

Máy chủ DNS Master sẽ làm primary của tất cả các zone (bao gồm các zone có yêu cầu ký DNSSEC và các zone không yêu cầu ký), từ DNS Master sẽ chia làm 2 nhánh, trong đó một nhánh sẽ trực tiếp đồng bộ (zone transfer) những zone không ký đến các DNS Slave, và một nhánh sẽ thực hiện đồng bộ các zone dùng để ký đến DNSSEC-Signer (DNSSEC-Signer lúc này chính là master của các DNS Slave đối với những zone được ký DNSSEC), từ đó zone transfer về các Slave.

3.5. Xây dựng hệ thống thử nghiệm

Hệ thống thử nghiệm có thể được xây dựng theo nhiều cách khác nhau. Tuy nhiên, về cơ bản thì bao gồm các bước sau:

Lưu ý: Phần này sẽ hướng dẫn xây dựng hệ thống thử nghiệm DNSSEC đối với hệ thống DNS sử dụng thuần phần mềm BIND.

3.5.1. Chuẩn bị dữ liệu zone thử nghiệm:

- ***Nội dung:*** Chuẩn bị các dữ liệu zone thử nghiệm cho hệ thống DNS Hosting Provider
- ***Mục đích:*** Chuẩn bị dữ liệu zone thử nghiệm trên hệ thống DNS Hosting Provider, phục vụ triển khai thử nghiệm DNSSEC trong hệ thống Lab trước khi triển khai trên hệ thống chính thức.
- ***Yêu cầu:*** Cấu hình đầy đủ các zone giống trên hệ thống DNS Hosting:
- ***Thực hiện:***
    - Lập danh sách các zone sẽ thử nghiệm (Bao gồm cả zone thuận và zone ngược): zone1, zone2, zone3 …
    - Dữ liệu trong các zone, sử dụng một trong hai cách:
        - Sử dụng dữ liệu thật trên DNS Hosting.
        - Sử dụng dữ liệu mô phỏng.

3.5.2. Triển khai máy chủ thử nghiệm:

Triển khai hệ thống máy chủ DNS thử nghiệm mô phỏng hệ thống DNS Hosting đang được sử dụng hoạt động chính thức.

- Lưu ý bổ sung thêm log DNSSEC như sau:

Trong trường Option của file ***/etc/named.conf***, bổ sung thêm nội dung sau:

```
channel dnssec_log {
       file "logs/dnssec.log" size 5m versions 2;
       print-time yes;
       print-category yes;
       print-severity yes;
       severity info;
       };
       category dnssec { dnssec_log; };
```

3.5.3. Lập danh sách các zone sẽ thử nghiệm ký DNSSEC:

Trong trường hợp hệ thống thật có quá nhiều zone: Có thể chỉ cần triển khai trên mô hình LAB các zone sẽ sử dụng để ký và một vài zone khác để kiểm tra trạng thái hoạt hoạt động của hệ thống.

Kiểm tra đảm bảo hệ thống thử nghiệm hoạt động tốt với các zone dự kiến ký DNSSEC.

- Lưu lại các thông tin sau:
    - Danh sách các máy chủ thử nghiệm.

STT	Tên máy chủ	Địa chỉ IPv4 / IPv6	Ghi chú
1	DNS Lab Master		
2	DNS Lab Slave		

Bảng 4: Danh sách các máy chủ thử nghiệm

    - Danh sách các Zone thử nghiệm, file chứa dữ liệu thử nghiệm

STT	Zone thử nghiệm	Tên file dữ liệu	Ghi chú

1	thunghiem1.vn	/var/named/thunghiem1	
2	thunghiem2.vn	/var/named/thunghiem2	
3	labdnssec.vn	…..	
4			

Bảng 5: Danh sách các zone, tập tin dữ liệu thử nghiệm

- Kết quả kiểm tra hệ thống thử nghiệm:

STT	Nội dung kiểm tra	Kết quả kiểm tra	Ghi chú
1	Phiên bản BIND		
2	Hoạt động của DNS Master		
3	Hoạt động của DNS Slave		
4	Truy vấn bản ghi của các Zone thử nghiệm		

Bảng 6: Kết quả kiểm tra hệ thống thử nghiệm

3.6. Tiến hành thử nghiệm

Phần này sẽ hướng dẫn và cung cấp các thông tin để thiết lập, cấu hình triển khai DNSSEC trên hệ thống máy chủ DNSSEC của các nhà cung cấp dịch vụ DNS Hosting. Ký DNSSEC sẽ thêm vào các bản ghi tài nguyên mới (DNSKEY, RRSIG, NSEC/NSEC3) và cần phải thực hiện cập nhật bản ghi DS lên zone cha (Parent Zone) để hoàn thành chuỗi tin cậy (Chain of trust).

3.6.1. Tạo khóa và quản lý khóa DNSSEC&BIND:

3.6.1.1. Giới thiệu về các loại khóa trong công nghệ DNSSEC

- Trong công nghệ DNSSEC có 02 loại khóa:

  - Zone Signing Key (ZSK): được sử dụng để ký cho tất cả các dữ liệu thẩm quyền trong một zone.
  - Key Signing Key (KSK): được dùng để ký bản ghi DNSKEY trong một zone.
- Key Signing Key (KSK):
  - KSK dùng để ký bản ghi DNSKEY trong một zone.
  - KSK luôn có odd flag là 257.
  - Khi KSK thay đổi, bản ghi DS trong parent zone phải được update.
  - KSK thường được tạo với kích thước lớn để chống lại các tấn công brute force.
  - KSK thường có thời gian sống (lifetime) dài
- Zone Signing Key (KSK):
  - ZSK được dùng để ký cho tất cả các bản ghi trong zone (bao gồm cả DNSKEY). Tuy nhiên không ký cho các bản ghi NS chuyển giao và glue records.
  - ZSK luôn có odd flag là 256.
  - Khi ZSK thay đổi, không cần thiết phải thay đổi bản ghi DS trên parent zone.
  - ZSK thường có thời gian sống ngắn hơn, và được "rolled" nhiều hơn.

3.6.1.2. Tổng quan

- ***Nội dung:*** Tạo khóa và quản lý khóa DNSSEC
- ***Mục đích:*** Tạo cặp khóa ZSK, KSK cho từng zone; các tham số tạo khóa; cách thức lưu trữ và quản lý các cặp khóa tương ứng với từng zone.
- ***Yêu cầu:*** Nắm rõ cách thức tạo các cặp khóa ZSK, KSK cho từng zone trên DNS Hosting Provider:

  - Câu lệnh tạo khóa với BIND.
  - Các tham số tạo khóa.
  - Quản lý và lưu trữ các cặp khóa tương ứng với từng zone.

- **Một số khuyến nghị:** Nghiên cứu và lựa chọn các tham số của cặp khóa ZSK, KSK; khuyến cáo nên sử dụng các thông số của các khóa như sau:

    - ZSK (lifetime: 3 months, key size: 1024 bits; Algorithm: RSA/SHA-256)
    - KSK (lifetime: 1 year, key size: 2048 bits; Algorithm: RSA/SHA-256)

3.6.1.3. Hướng dẫn các bước thực hiện:

- ***Tạo các khóa với BIND.***

Với các tham số khóa như sau:

ZSK: *RSASHA256, 1024 bits*

KSK: *RSASHA256, 2048 bits*

Tạo khóa ZSK

```
#dnssec-keygen -r /dev/urandom -a RSASHA256 -b 1024
labdnssec.vn
```

Tạo khóa KSK

```
#dnssec-keygen -r /dev/urandom -f ksk -a RSASHA256 -b 2048
labdnssec.vn
```

- ***Quản lý và lưu trữ các cặp khóa tương ứng với từng zone.***

Tùy thuộc vào việc quản lý khóa, toàn bộ các cặp khóa được lưu trữ trong thư mục "*/var/namedb/master/"*

Hoặc có thể lưu riêng theo từng thư mục cho từng zone để quản lý khóa một cách dễ dàng:

"/var/namedb/keys/zonename/"

Sau khi kết thúc quá trình tạo khóa, sẽ tạo ra một cặp khóa tương ứng tồn tại dưới dạng file: Private key (*.private*) và Public Key (*.key*)

```
Klabdnssec.vn.+008+18048.key      ;          ZSK Public key
Klabdnssec.vn.+008+18048.private  ;          ZSK Private key
Klabdnssec.vn.+008+21112.key      ;          KSK Public key
Klabdnssec.vn.+008+21112.private  ;          KSK Private key
```

3.6.2. Ký zone DNSSEC trên hệ thống DNS Hosting Provider:

3.6.2.1. Tổng quan:

- ***Nội dung:*** Thực hành ký zone DNSSEC trên hệ thống DNS Hosting Provider theo phương pháp ký bằng tay – manual.
- ***Mục đích:*** Sử dụng cặp khóa ZSK, KSK ở trên để thực hiện chức năng ký cho các zone trên hệ thống DNS Hosting Provider.
- ***Yêu cầu:*** Nghiên cứu, nắm rõ các bước thực hiện ký zone DNSSEC trên DNS Hosting Provider:
    - Thực hành theo các bước thực hiện ký DNSSEC cho zone
    - Phương pháp kiểm tra việc ký zone trên máy chủ DNS.
        - Bằng công cụ DIG.
        - Dựa trên thông tin log file:

3.6.2.2. Hướng dẫn thực hiện:

- ***Bước 1: Chèn khóa công khai DNSKEY vào trong tập tin dữ liệu zone***

Mở tập tin dữ liệu zone (db.labdnssec.vn) và chèn thông tin của các khóa vào cuối bằng các dòng như sau:

```
#vi db.labdnssec.vn
$INCLUDE
"/var/namedb/keys/labdnssec_vn/Klabdnssec.vn.+008+18048.key" ;
ZSK Public key
```

```
$INCLUDE
"/var/namedb/keys/labdnssec_vn/Klabdnssec.vn.+008+21112.key"
; KSK Public key
```

- ***Bước 2: Thực hiện ký zone sử dụng khóa bí mật***

```
# dnssec-signzone -o labdnssec.vn -k Klabdnssec.vn.+008+21112
db.labdnssec.vn Klabdnssec.vn.+008+18048
```

- ***Bước 3: Kiểm tra các thông tin sau khi thực hiện ký bằng tay***

Sau khi quá trình ký kết thúc, đối với zone được ký sẽ tạo ra một zone file dưới dạng *.signed.*

```
[root@auth1 ~]# ls /var/namedb/master/
db.labdnssec.vn
db.labdnssec.vn.signed
```

Trong nội dung tập tin dữ liệu zone sau khi thực hiện ký DNSSEC sẽ thêm thông tin các bản ghi tài nguyên DNSKEY, RRSIG, NSEC,…

```
[root@auth1 ~]# more /var/namedb/master/db.labdnssec.vn.signed
; File written on Tue Aug 26 15:21:05 2014
; dnssec_signzone version 9.9.5-P1
labdnssec.vn.               43200   IN SOA  dns1.labdnssec.vn.
postmaster.labdnssec.vn. (
                                            2014053001
      serial
                                            1800       ;
      refresh (30 minutes)
                                            900        ;
      retry (15 minutes)
                                            604800     ;
      expire (1 week)
                                            5400       ;
      minimum (1 hour 30 minutes)
                                            )
                           43200    RRSIG   SOA 8 2 43200 (
                                            20140925072105
      20140826072105 18048 labdnssec.vn.

      YCqtMXPExrjyb/8fuL4GbYXS0YvHuoNMz/2U
```

```
      cSBAvt67FTId2PMFIgRpDLn4sgaGfomwA9bd

      CChlVIliXOtmMOwysguhzHn36Ccw6JFCBzT2

      taWB+xbJYIoGTXOSSS4J62pEuLSRgwItWKnb

      MDl+SedtRiqpqHw8MYuLiTuS/ic= )
                              43200   NS
      dns1.labdnssec.vn.
                              43200   NS
      dns2.labdnssec.vn.
                              43200   RRSIG   NS 8 2 43200 (
                                              20140925072105
      20140826072105 18048 labdnssec.vn.

      cFKlIy0Fczl3bT/B0waGc1bsjAb29MHQHxj3

      jKvhEUZim/uzwqnmyksbfjw1Ru6bGrjmZbIm

      reOdUWmylpgxT57xKipFVscYZiXssRUGgd3E

      FHAO2PYjXpIjA9gyM7DxmhdPB5yqc2Hb9wVo
      ...
```

- ***Bước 4: Khai báo sử dụng zone đã ký DNSSEC***

Chỉnh sửa thông tin cấu hình zone trong file cấu hình "*named.conf*" như sau:

```
[root@auth1 labdnssec.vn]# vi /etc/named.conf
zone " labdnssec.vn " in {
                type master;
                file "db. labdnssec.vn.signed";
                allow-transfer {key k138-139; };
                };
```

- ***Bước 5: Thực hiện khởi động lại dịch vụ named để áp dụng cấu hình mới.***

```
# service named restart
Hoặc
# /etc/init.d/named stop
# /etc/ini.d/named start
```

- ***Bước 6: Kiểm tra thông tin zone đã được ký trên hệ thống DNS.***
    - Bằng công cụ DIG tool (thực hiện truy vấn tên miền và kèm theo tham số trường +dnssec):

```
[root@auth1 labdnssec.vn]# dig @203.119.8.138
www.labdnssec.vn +dnssec

; <<>> DiG 9.9.5-P1 <<>> @203.119.8.138 www.labdnssec.vn
+dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47526
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3,
ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.labdnssec.vn.              IN      A

;; ANSWER SECTION:
www.labdnssec.vn.       43200   IN      A       192.168.1.85
www.labdnssec.vn.       43200   IN      RRSIG   A 8 4 43200
20141007072955 20140907072955 35766 labdnssec.vn.
kiqXpgaHwm6Tc1SBRqsJNV7Vst5lbPP0FMJJnc4IgSae4Vh/s0J1HcBf
SNlEP1XX2ZEv26+pOHjZx+bnVmeygbhDB7KlDvXnyWrXBCZRC3EBiyK2
S0OnNjsQvAFt3j5w+lFR2Urq6u1vZEhCdRxzxnT54GQyhl7Sh30YySDn LCo=
    -
;; AUTHORITY SECTION:
labdnssec.vn.           43200   IN      NS
dns2.vnnic.vn.
labdnssec.vn.           43200   IN      NS
dns1.vnnic.vn.
labdnssec.vn.           43200   IN      RRSIG   NS 8 3 43200
20141007072955 20140907072955 35766 labdnssec.vn.
ILwFhGBjiZ07Y3r3l+WZjZH6Km4fn32mSuoGFGY+OA/90fhaB/DCgVfq
vZ3ESYE0GLyDPnO5UeT35TVDgIx11DqZgShI8Z1EgDJqGfNM9fL27F/X
Ew4fV2tr8WNxq6zMhJ4Cl+AsHkLelr3FdcsDOfLciimwqeoOcCXpHAHI Jag=
;; ADDITIONAL SECTION:
dns1.vnnic.vn.          43200   IN      A       192.168.1.108
dns1.vnnic.vn.          43200   IN      AAAA
21aa:af6:0:2::108
dns2.vnnic.vn.          43200   IN      A
192.168.36.108
dns2.vnnic.vn.          43200   IN      AAAA
21aa:af6:c000:2::108
```

```
dns1.vnnic.vn.          43200   IN      RRSIG   A 8 3 43200
20140930221925 20140831221925 18048 vnnic.vn.
haSwk5xWrsqFI5xp2wNVdRuH5mztltItvafLNmcYGKa+D0ZxrORkOLxl
F4lZgkgT8bLaFFfpFIWY0Tajfd/KI9WZvVNt8OgmR6ntDf8770f5vO6s
4dflAQCF8zv8hVgztTmmFNoUSN7IM3RYgwhn3qM5B455fIB+amnvyoqw
ZSY==
...
```

3.6.3. Ký zone DNSSEC với tính năng Inline signing:

3.6.3.1. Tổng quan:

Đối với các phiên bản Bind từ 9.9 trở lên, sẽ hỗ trợ tính năng Inline Signing.

- ***Nội dung:*** Ký zone DNSSEC với tính năng Inline Signing của BIND
- ***Mục đích:*** Ký zone DNSSEC tự động với tính năng Inline signing của BIND (phiên bản 9.9 trở lên)
- ***Yêu cầu:*** Thực hiện lại các bước trên sử sụng Inline Signing

Thực hiện lại với hai trường hợp Inline Signing:

- Inline Signing "Box-to-box"
- Inline Signing "Bump in the wire"

Nắm rõ các tiến trình diễn ra trong quá trình ký tự động Inline Signing:

- Tần suất, chu kỳ ký lại
- Khả năng quản lý, cập nhật zone khi có bản ghi mới.
- Theo dõi việc ký tự động Inline signing: log file,…

3.6.3.2. Hướng dẫn thực hiện:

Có thể sử dụng lại các khóa đã tạo ở phương pháp trên, hoặc có thể tạo lại các cặp khóa mới cho zone.

- ***Bước 1: Cấu hình Inline signing cho zone***

```
zone "labdnssec.vn" in {
            type master;
            auto-dnssec maintain;
            inline-signing yes;
            key-directory "/var/namedb/keys/labdnssec_vn";
            file "db.labdnssec.vn";
```

```
        };
```

- ***Bước 2: Thực hiện tạo lại các khóa ZKS và KSK:***

```
# dnssec-keygen -r /dev/urandom -a rsasha256 -b 1024
labdnssec.vn
# dnssec-keygen -r /dev/urandom -f ksk -a rsasha256 -b 2048
labdnssec.vn
```

- ***Bước 3: Thông tin các khóa mới vừa được tạo:***

```
Klabdnssec.vn.+008+05395.key
Klabdnssec.vn.+008+05395.private
Klabdnssec.vn.+008+18435.key
Klabdnssec.vn.+008+18435.private
```

- ***Bước 4: Khởi động lại dịch vụ named***

Nhằm mục đích áp dụng cấu hình mới thực hiện ký tự động – Inline signing:

```
# service named restart
Hoặc
# /etc/init.d/named stop
# /etc/ini.d/named start
```

Sau khi quá trình ký tự động – Inline signing hoàn tất, sẽ tạo ra các tập tin dưới dạng mã hóa như sau:

```
db.labdnssec.vn.jbk
db.labdnssec.vn.jnl
db.labdnssec.vn.signed
db.labdnssec.vn.signed.jnl
```

- ***Bước 5: Kiểm tra thông tin zone đã được ký trên máy chủ DNS***
  - Bằng câu lệnh named-checkzone

```
[root@auth1 master]# named-checkzone -D -f raw -o -
labdnssec.vn /data/namedb/master/db.labdnssec.vn.signed |
less
zone labdnssec.vn/IN: loaded serial 2014090801 (DNSSEC
signed)
OK
labdnssec.vn.                                    43200 IN SOA
dns1.vnnic.vn. postmaster.vnnic.vn. 2014090801 1800 900
604800 5400
```

```
labdnssec.vn.                                          43200 IN
RRSIG    SOA 8 2 43200 20141008044419 20140908034419 18435
labdnssec.vn.
kQUXc+71JSakcR74scINbG4sMTEZgzmW4ZJmEwCG/FfDfw0+vS22HOAr
oKPie5Y34tF+S6xmbEMKsoaJtOFImdXa027qFcun+O+3oM4PeCYQ3LWt
I1UFByLE8pIbr7/MY9WwMmeVhg5WMQ2VXdkOEZwZteNjkTlBPZ8Xm9eU GKw=
labdnssec.vn.                                          43200 IN NS
dns1.vnnic.vn.
labdnssec.vn.                                          43200 IN NS
dns2.vnnic.vn.
labdnssec.vn.                                          43200 IN NS
dns3.vnnic.vn.
labdnssec.vn.                                          43200 IN
RRSIG    NS 8 2 43200 20141008034401 20140908033104 18435
labdnssec.vn.
m6SVwAHJ8BaqSDSjNmyzAHZE44dTlpwQRTpeBFPQGlhC2zlLqylpe+JX
ZIkMZOUEdXf8Kb17iGe3ht0ukl9wcS96JPQaGnwKXFkr2TH3NSOCBvh3
E9tTV9k/lPZR/9iq5VcNMl+dSbuY7PsJaDOoG8bOyZIQCuknd6ovpmPh ffA=
labdnssec.vn.                                          43200 IN A
192.168.1.85

labdnssec.vn.                                          43200 IN

RRSIG    A 8 2 43200 20141008034401 20140908033104 18435

labdnssec.vn.

NIpswfIc/d6j4fiupjTSpQvzbtt+AHlKwDbJPaTTyLd56QFGtHbwYROx

BwaZKYLxAKDrU0GG8grEH3xiRLZBrYkFoO1CGAU4a7MbJepqAb4/vEPI
```

- Bằng công cụ DIG tool

```
[root@auth1 master]# dig @203.119.8.138 www.labdnssec.vn
+dnssec

; <<>> DiG 9.9.5-P1 <<>> @203.119.8.138 www.labdnssec.vn
+dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10738
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 3,
ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.labdnssec.vn.                      IN      A
```

```
;; ANSWER SECTION:
www.labdnssec.vn.          43200   IN      CNAME
webproxy.vnnic.net.vn.
www.labdnssec.vn.          43200   IN      RRSIG   CNAME 8 3
43200 20141008034401 20140908033104 18435 labdnssec.vn.
T8Uf3/nQhTCkYRpVDe5CzyUSguy3rIXxMMz1Y32+I5S66SncULjN3Woq
0imGfmCwe4iYnEGnHmaNhyI5vLPfqJ6jrkkHK02asmXFemvBwCG7kt0D
wheHMY6AAWh9lAmkvl5nBNUMsNULIKoKdqH7jOLMcc8b8aavLM+T7Pna qLA=
webproxy.vnnic.net.vn.  43200   IN      A       203.162.57.28
webproxy.vnnic.net.vn.  43200   IN      RRSIG   A 8 4 43200
20141007072955 20140907072955 35766 vnnic.net.vn.
tUJPvgFbIZIcou19glijIuqWIU4Sw4N/3GPM09xQcX24WyoceahDz+qn
a24Dx9dZItVzwQ95kP9425MpqOTLxpu/x9E4zg3W0e6zC31gF3JsNSJB
tgnsMN7YncWplDN3oDh4sjBGByR//dnEYmIW1ITcpLkISfFv1undSjsZ +tg=

;; AUTHORITY SECTION:
vnnic.net.vn.           43200   IN      NS
dns1.vnnic.vn.
vnnic.net.vn.           43200   IN      NS
dns2.vnnic.vn.
vnnic.net.vn.           43200   IN      RRSIG   NS 8 3 43200
20141007072955 20140907072955 35766 vnnic.net.vn.
ILwFhGBjiZ07Y3r3l+WZjZH6Km4fn32mSuoGFGY+OA/90fhaB/DCgVfq
vZ3ESYE0GLyDPnO5UeT35TVDgIx11DqZgShI8Z1EgDJqGfNM9fL27F/X
Ew4fV2tr8WNxq6zMhJ4Cl+AsHkLelr3FdcsDOfLciimwqeoOcCXpHAHI Jag=

;; ADDITIONAL SECTION:
   dns1.vnnic.vn.          43200   IN      A
   192.168.1.108
dns1.vnnic.vn.          43200   IN      AAAA
21aa:af6:0:2::108
dns2.vnnic.vn.          43200   IN      A
192.168.36.108
dns2.vnnic.vn.          43200   IN      AAAA
21aa:af6:c000:2::108
dns1.vnnic.vn.          43200   IN      RRSIG   A 8 3 43200
20140930221925 20140831221925 18048 vnnic.vn.
haSwk5xWrsqFI5xp2wNVdRuH5mztltItvafLNmcYGKa+D0ZxrORkOLxl
F4lZgkgT8bLaFFfpFIWY0Tajfd/KI9WZvVNt8OgmR6ntDf8770f5vO6s
4dflAQCF8zv8hVgztTmmFNoUSN7IM3RYgwhn3qM5B455fIB+amnvyoqw ZSY=
dns1.vnnic.vn.          43200   IN      RRSIG   AAAA 8 3
43200 20140930221925 20140831221925 18048 vnnic.vn.
r1V2Ywf8dv4BWfzzXipOTLqxZvnZmzlEP9Ul09wPCIQg83MJy3aHGq11
+wbfifSUAvp/bqfGADGQ6JVqXvTiPFW5UrvhALJscVriIkpbJQO7PHlg
x+XB3z2dSzZWUcbq66Ufpd43waFcbiN7k2GsfTclFK97fEQ6FiKCY62h rNY=
dns2.vnnic.vn.          43200   IN      RRSIG   A 8 3 43200
20140930221925 20140831221925 18048 vnnic.vn.
XEN8rPHiZH8pkx4RzNoJJSsmRZHRIciLQYwo2JttILa6JXy1Gi6CJMHJ
IhZY9xLY/llHILyLmw303NJU7XX9fh6yAv3+fKmsj9dZI1Q0Icu9QQJg
```

```
WBZ4lg+H0cejfRaNQrGwfQBduwj8fdcG3yPmiyfe9E9B8Du4jdXfvwVL nlw=
dns2.vnnic.vn.          43200   IN      RRSIG   AAAA 8 3
43200 20140930221925 20140831221925 18048 vnnic.vn.
IYlrEu81VSky1MfB7Orub5tWN/qaSuNf/3bS0JbgZQtACiZ+pakH2CTW
BmcSKSUpXG0crhoLy8NavL0P881q4b9CnR94jK2Y7y3jaEahOUdr5dVh
SLvsIjuESObW+adQnIzwf9W/P5h8xUY64PpAVLgs9C/9xIiBBf03QhEd aFg=

;; Query time: 1 msec
;; SERVER: 203.119.8.138#53(203.119.8.138)
;; WHEN: Mon Sep 08 23:55:06 ICT 2014
;; MSG SIZE  rcvd: 1410
```

3.6.4. Tạo bản ghi DS và xác minh

Sau khi các zone đã được ký cần đảm bảo chính xác các thông tin của zone trước khi tạo, cập nhật và gửi bản ghi DS lên các NĐK để hoàn thành chuỗi xác thực.

- Đầu tiên cần tạo bản ghi DS bằng các phương pháp sau:

  Tạo bản ghi DS bằng lệnh dnssec-dsfromkey với các thuật toán (RSA/SHA-1 và RSA/SHA-256; đây là hai thuật toán phổ biến nhất hiện nay được sử dụng cho mã hóa DNSSEC)

```
# cd /var/namedb/keys/labdnssec_vn
# dnssec-dsfromkey -a SHA-1 Klabdnssec.vn.+008+18435.key
labdnssec.vn. IN DS 18435 8 1
59194A835ACD78D25D538D5F35CA043A8F3F4446
# dnssec-dsfromkey -a SHA-256 Klabdnssec.vn.+008+18435.key
labdnssec.vn. IN DS 18435 8 2
2A5F1DF55D5E64CBD7BCFE1EFA6E9586AF335FA56A2473296E975B89AFD31
E11
```

  Hoặc có thể sử dụng công cụ DIG tool kết hợp với lệnh dnssec-dsfromkey để lấy thông tin bản ghi DS của zone được ký:

```
$ dig @203.119.8.138 labdnssec.vn. DNSKEY | dnssec-dsfromkey
-f - labdnssec.vn
```

```
example.com. IN DS 18435 8 1
59194A835ACD78D25D538D5F35CA043A8F3F4446
labdnssec.vn. IN DS 18435 8 2
2A5F1DF55D5E64CBD7BCFE1EFA6E9586AF335FA56A2473296E975B89AFD31
E11
```

- Để xác minh thông tin bản ghi DS, sử dụng công cụ "delv" để mô phỏng quá trình xác thực chuỗi tin cậy.

Tạo ra một bản sao cho khóa công khai (public) của KSK.

```
# cp
/var/namedb/keys/labdnssec_vn/Klabdnssec.vn.+008+18435.key
/tmp/labdnssec.key
```

Các thông tin của khóa công khai sẽ bao gồm thông tin được rút gọn như sau:

```
# cat
/var/namedb/keys/labdnssec_vn/Klabdnssec.vn.+008+18435.key
...
labdnssec.vn. IN DNSKEY 257 3 8 AwEAAcWDps...lM3NRn/G/R
```

Chỉnh sửa thông tin trong bản sao của khóa như sau:

```
# cat /tmp/labdnssec.key
trusted-keys {
    labdnssec.vn. 257 3 8 "AwEAAcWDps...lM3NRn/G/R";
};
```

Sử dụng lệnh ***"delv"*** để thực hiện kiểm tra

```
$ delv @203.119.8.138 -a /tmp/labdnssec.key
+root=labdnssec.vn labdnssec. SOA +multiline
; fully validated
```

3.7. Đánh giá kết quả thử nghiệm, đề xuất triển khai chính thức

Sau khi thực hiện việc thử nghiệm thành công, đơn vị cần đánh giá lại toàn bộ quá trình thử nghiệm, tài liệu hóa các khâu và tiến hành đề xuất kế hoạch nâng cấp hệ thống một cách chi tiết.

Tài liệu kế hoạch nâng cấp, phải đảm bảo các nội dung sau:

Mục tiêu:

Cần đánh giá được mục tiêu của việc nâng cấp, chuyển đổi hệ thống.

Mô hình triển khai, nguyên lý hoạt động:

Xác định mô hình hệ thống sẽ triển khai, nguyên lý hoạt động của hệ thống mới, cũng như các thành phần liên quan.

Kế hoạch thực hiện:

Phải chia thành từng giai đoạn rõ ràng, mỗi giai đoạn cần xác định rõ nội dung, thời gian, kết quả đạt được và người thực hiện.

Danh sách các trang thiết bị cần thiết:

Xác định rõ ràng các trang thiết bị cần đáp ứng để có thể triển khai. Ghi rõ nguồn gốc của các trang thiết bị, trong trường hợp chưa có thì cần đề xuất điều chuyển hoặc mua mới.

Đồng thời cũng phải xác định được các thiết bị dư thừa sau triển khai sẽ sử dụng vào việc nào, ở đâu v.v.

Các yêu cầu khi triển khai:

- Phần này cần xác định rõ các yêu cầu khi triển khai. Một số yêu cầu thường gặp như:
- Đánh giá rủi ro có thể gặp phải khi nâng cấp hệ thống, từ đó đưa ra được các biện pháp giảm thiểu, phòng ngừa rủi ro một cách thích hợp.

- Các yêu cầu cần đáp ứng: Gián đoạn tối đa là bao nhiêu phút, các cam kết dịch vụ cần đảm bảo v.v.
- Kịch bản roll back khi có vấn đề xảy ra trong quá trình triển khai, nâng cấp, cần phải trở lại hệ thống cũ.

Các nội dung khác:

- ***Check list:*** Đây là một phần hết sức quan trọng, cần xây dựng check list cho tổng thể kế hoạch, check list cần đảm bảo rõ ràng, chi tiết, đầy đủ nội dung cũng như các thông số đo lường kết quả. Ngoài ra có thể bổ sung các tài liệu hướng dẫn kiểm tra Check list.

  Trong từng giai đoạn, phải đảm bảo Check list của giai đoạn trước hoàn thành thì mới triển khai giai đoạn tiếp theo

- ***Check list trước triển khai:*** Bao gồm các nội dung công việc cần chuẩn bị trước triển khai cụ thể, tiến độ thực hiện và kết quả chuẩn bị các công việc. Đảm bảo đã sẵn sàng và tiến hành triển khai.
- ***Check list trong triển khai:*** Liệt kê rõ ràng từng hạng mục cần hoàn thành, các kết quả cần đạt được, và phải tiến hành kiểm tra xác nhận và thống nhất các hạng mục trước khi tiến hành triển khai chuyển đổi chính thức.
- ***Check list sau triển khai:*** Thông thường check list sau triển khai sẽ phải có đầy đủ các nội dung kiểm tra tính hoạt động ổn định của hệ thống. Bên cạnh đó phải đảm bảo các quy trình, tài liệu liên quan được cập nhật, ban hành.
- ***Các hệ thống liên quan:*** Một số hệ thống liên quan đã liệt kê trong phần kế hoạch thực hiện, nhưng cần thể hiện chi tiết nội dung tại đây: Ví dụ như danh sách các Rule Firewall cần mở, danh sách các cấu hình máy chủ cần thay đổi, v.v.

3.8. Thực hiện triển khai hệ thống để chuyển đổi

Sau khi kế hoạch chuyển đổi được thống nhất, đơn vị cần tiến hành thực hiện theo đúng các hạng mục trong kế hoạch, kèm theo đó là kiểm tra đầy đủ theo check list.

Theo mô hình đề xuất, thì để triển khai chính thức hệ thống hỗ trợ DNSSEC, đơn vị sẽ phải thực hiện các công việc sau:

3.8.1. Kiểm tra khả năng hỗ trợ DNSSEC của hệ thống hiện tại:

- Đối với các hệ thống hiện tại đang hoạt động, cần cấu hình hệ thống đảm bảo hỗ trợ DNSSEC: enable dnssec
- Kiểm tra truy vấn từ bên ngoài xem có sẵn sàng hỗ trợ TCP/UDP/53 qua IPv4/IPv6.
    - Có thể sử dụng một số công cụ online để kiểm tra:

      http://dnscheck.ripe.net/;

      http://dnscheck.pingdom.com
- Kiểm tra đảm bảo các hệ thống Firewall đã hỗ trợ triển khai DNSSEC.

3.8.2. Triển khai máy chủ DNSSEC Signer:

- Cài đặt, triển khai máy chủ, cấu hình phần mềm BIND: Tương tự nội dung đã hướng dẫn trong phần xây dựng hệ thống thử nghiệm.
- Cấu hình đưa vào hệ thống giám sát.
- Xác định các tên miền sẽ ký DNSSEC.
- Cấu hình làm Slave của máy chủ DNS Master đối với các tên miền sẽ ký DNSSEC
- Cấu hình làm master cho các máy chủ slave đối với các tên miền ký DNSSEC.

3.8.3. Cấu hình máy chủ DNS Master:

- Trên DNS Master sẽ phải cấu hình cho phép zone transfer tên miền được ký DNSSEC xuống DNSSEC Signer.

3.8.4. Kiểm tra trên DNSSEC Signer:

- Kiểm tra quá trình zone transfer các zone sẽ được ký DNSSEC từ DNS Master xuống.

- Tạo khóa cho tên miền sẽ ký DNSSEC.
- Ký DNSSEC cho tên miền cần ký.
- Kiểm tra quá trình ký thành công hay không *(Chi tiết cách kiểm tra sẽ nêu ở phần sau).*

Sau khi ký thành công trên máy chủ DNSSEC Signer, do chưa thay đổi cấu trúc hệ thống, hệ thống vẫn hoạt động bình thường theo mô hình cũ, nên không cần thiết phải thực hiện ngay bước chuyển đổi chính thức. Đơn vị cần thực hiện đầy đủ các bước kiểm tra, đảm bảo sẵn sàng chuyển đổi.

Do tính chất của các DNS Hosting Provider quản lý với số lượng lớn các zone tên miền và thường xuyên cập nhật thay đổi các thông tin về tên miền ; khi triển khai áp dụng DNSSEC vào hệ thống cũng sẽ phải thực hiện nhiều hơn các thao tác về tạo hay thay khóa. Do vậy trên máy chủ DNSSEC Signer, nên cập nhật lên phiên bản BIND 9.11 (phiên bản mới nhất tính đến thời điểm hiện tại) để có thể sử dụng tính năng mới DNSSEC Key Manager trong việc tạo, vận hành và quản lý khóa DNSSEC một cách thuận tiện và tránh các sai sót. (Tham khảo phụ lục 1.2)

3.9. Chuyển đổi chính thức

3.9.1. Cấu hình các máy chủ Slave:

- Sau khi đã ký thành công trên DNSSEC Signer và đảm bảo các kiểm tra đã hoàn thành. Trên các DNS Slave, đối với các tên miền ký DNSSEC, chỉ cần đổi địa chỉ máy chủ DNS Master thành địa chỉ của máy chủ DNSSEC Signer.

3.9.2. Kiểm tra hoạt động của hệ thống.

- Kiểm tra đảm bảo quá trình zone transfer các dữ liệu tên miền ký DNSSEC được chuyển xuống các DNS Slave.
- Kiểm tra truy vấn bản ghi DNSKEY của các tên miền ký DNSSEC:
    - Từ trong mạng: Sử dụng lệnh dig
    - Từ ngoài mạng, sử dụng các trang kiểm tra online: http://dnsviz.net/

3.9.3. Gửi và cập nhật bản ghi DS lên zone cha (Parent Zone)

Sau khi thực hiện thành công các bước trên, và bây giờ cần gửi cập nhật bản ghi DNS và một số thông tin lên zone cha (Parent Zone) để hoàn thành chuỗi tin cậy. Các định dạng và các phương thức tải lên được quy định bởi tổ chức quản trị zone cha, do vậy cần liên hệ với các tổ chức NĐK để lấy thêm các thông tin làm thế nào để tải hay cập nhật thông tin của các zone đã được ký lên các zone cha.

Trước khi cập nhật gửi thông tin lên zone cha, phải đảm bảo chắc chắn rằng zone mới được ký đã được đồng bộ đến tất cả các máy chủ trong hệ thống DNS.

Bản ghi DS được tạo ra bằng cách sử dụng câu lệnh ***"dnssec-dsfromkey"***

```
# dnssec-dsfromkey -a SHA-256 Kexample.vn.+008+06817.key
example.vn. IN DS 6817 8 2
2A5F1DF55D5E64CBD7BCFE1EFA6E9586AF335FA56A2473296E975B89AFD31E11
```

Kiểm tra thông tin bản ghi DS sau khi được cập nhật trên zone cha bằng cách:

```
$ dig example.vn. DS

; <<>> DiG 9.10.1 <<>> example.vn. DS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49949
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.vn.                IN   DS
```

```
;; ANSWER SECTION:
example.vn.  61179  IN   DS   28267 8 1
66D47CE4B4F551BE5EDA43AC5F3109E8C98E2FAE
example.vn.  61179  IN   DS   28267 8 2
71D9335416B7132519190A95685E18CBF478DCF4CA98867062777938F8FEAB89
```

3.9.4. Một số công cụ kiểm tra DNSSEC

3.9.4.1. Kiểm tra dữ liệu của khóa có trong zone sau khi ký

Một trong những cách để xem nếu như zone của bạn được ký kết, chính là kiểm tra sự hiện diện của các bản ghi DNSKEY trong zone đó. Bằng cách thực hiện công cụ ***"DIG Tool":***

```
# dig @192.168.1.13 example.vn. DNSKEY +multiline +noall +answer

; <<>> DiG 9.10.1 <<>> @192.168.1.13 example.vn. DNSKEY +multiline
+noall +answer
; (1 server found)
;; global options: +cmd
example.vn.                     300 IN DNSKEY 256 3 8 (
                    AwEAAclob7q+ccvDwaTVuMM2ddGIynWyMwaZlhFrU6cC
                    0qknWoPpkq0gIwTrYf3DJY+eIKPVHxrM+o2AoRIVhubG
                    jfv1bT5wTYrawZstS84ejCQ+ehA+8DxKyeWUEzW0ZMBe
                    OhyeG0cuQVK/p6Z1E096JLu0DjgbabLspequkw4M+HT7
                    ) ; ZSK; alg = RSASHA256; key id = 57009
example.vn.                     300 IN DNSKEY 257 3 8 (
                    AwEAAdQ2ctHx8VmryndiOgpchXPdj3NwxMeUvAre6uYI
                    5KELlFJUghTHrz+/CzEc8CXG8wwQ4ZvAey0FGV2nJAFC
                    ENMxoRiCz0oSiQQxryNhACd3RnE2/D7G+ShwlOM6w53E
                    wUJ/lsgu5UevSxFC+eA3fKeL3TWR44PH4iJQp9QmfW5v
                    7qG8Sic/HQvBGBdOGfFtHAl0a4jDPBi57imS4YsHcUYD
                    9bsWmhYWSHJKZ66+JnTiMS0nQM69YwBF43QfDKurs5R6
```

```
                    qPUDiBlaMCzSxmlaBU6fsI1Mu/yIU8w1ewy26a42rUTU
                    rPBC3Oa/zf9VQ8kpUrMZgJ7LEAA4xmR+qwWDh6U=
                    ) ; KSK; alg = RSASHA256; key id = 28267
```

Kết quả sẽ cho thông tin của 2 bản ghi DNSKEY đồng nghĩa với 2 khóa công khai của ZSK và KSK (nếu chính sách có sử dụng cả 2 loại khóa này để ký).

3.9.4.2. Kiểm tra chữ ký (Signatures) có trong Zone

Một cách khác để kiểm tra xem sự hiện diện của chữ ký có trong zone, nếu zone đó đã được ký, chữ ký chính là bản ghi RRSIG.

```
$ dig @192.168.1.13 example.vn. SOA +dnssec +multiline

; <<>> DiG 9.10.1 <<>> @192.168.1.13 example.vn. SOA +dnssec
+multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31466
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL:
1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;example.vn.            IN SOA

;; ANSWER SECTION:
example.vn.                     300 IN SOA ns1.example.vn.
dnsadmin.example.vn. (
                    2014102111 ; serial
```

```
                    10800       ; refresh (3 hours)
                    1080        ; retry (18 minutes)
                    2419200     ; expire (4 weeks)
                    900         ; minimum (15 minutes)
                    )
example.vn.                     300 IN RRSIG SOA 8 2 300 (
                    20141121122105 20141022112105 57009
example.vn.
                    NqPGNLkUs40Lg/qq7Fv+bgyCwVB4s9PsHQOK6p9ZWWk3
                    36z2Qz2WjM+Q19SlVBAPux9jijvcRcjGb6KREuxER9uX
                    wdVeiGx9a4X+PaO3qTqdkiXuGS2XkK1kBm1CgwhVHTYV
                    /nxVPrckU4/mpeUoFVjMnT49JkVJmgck63esPEU= )
```

3.9.4.3. Kiểm tra các Zone File

Theo mặc định DNS thông thường chỉ có 1 tập tin chứa dữ liệu của môt zone, nhưng sau khi thực hiện ký DNSSEC sẽ tự động sinh ra 03 tập tin bao gồm như sau:

```
# cd /etc/bind/db
# ls
example.vn.db  example.vn.db.jbk                    example.vn.db.signed
example.vn.db.signed.jnl
```

Trong đó:

- **.jbk**: tập tin tạm thời được sử dụng bởi named
- **.signed**: tập tin dữ liệu zone được ký ở dạng thô
- **.signed.jnl**: tập tin dạng journal của tập tin dữ liệu zone được ký.

3.9.4.4. Kiểm tra bằng các công cụ online

Sử dụng một số công cụ kiểm tra DNSSEC trên các Website để kiểm tra các thông tin xác thực dữ liệu tên miền sau khi ký:

- Verisign Labs DNSSEC Debugger: http://dnssec-debugger.verisignlabs.com/
- DNSViz: http://dnsviz.net/

Chỉ đạo biên soạn:

Ông Nguyễn Hồng Thắng – Phó Giám đốc VNNIC

Nhóm biên soạn:

Ông Nguyễn Trường Thành – Trưởng phòng Kỹ thuật

Ông Nguyễn Trung Kiên – Phó trưởng phòng Kỹ thuật

Ông Nguyễn Huy Bắc – Chuyên viên

Ông Nguyễn Văn Trí – Chuyên viên