|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**ĐỒ ÁN**

**BẢO MẬT THÔNG TIN**

**Đề tài: giới thiệu giao thức DNS security**

Ngành : **CÔNG NGHỆ THÔNG TIN**

Lớp : **18DTHB3**

Sinh viên thực hiện : **Phạm Vũ Khánh Toàn**

MSSV: 1811062015 Lớp: 18DTHB3

**Lê Thanh Bình**

MSSV: 1811061868 Lớp: 18DTHB3

**Nguyễn Hải Quân**

MSSV: 1811061822 Lớp: 18DTHB3

TP. Hồ Chí Minh, 2021

|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**ĐỒ ÁN**

**BẢO MẬT THÔNG TIN**

**Đề tài: giới thiệu giao thức DNS security**

Ngành : **CÔNG NGHỆ THÔNG TIN**

Lớp : **18DTHB3**

Sinh viên thực hiện : **Phạm Vũ Khánh Toàn**

MSSV: Lớp: 18DTHB3

**Lê Thanh Bình**

MSSV: 1811061868 Lớp: 18DTHB3

**Nguyễn Hải Quân**

MSSV: Lớp: 18DTHB3

TP. Hồ Chí Minh, 2021

**NHẬN XÉT CỦA GIẢNG VIÊN**

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

Mục lục

[LỜI NÓI ĐẦU 5](#_Toc70578225)

[CHƯƠNG 1: GIỚI THIỆU CHUNG VỀ DNSSEC 6](#_Toc70578226)

[1.1. Hệ thống tên miền (DNS – Domain name system) 6](#_Toc70578227)

[1.1.1. Định nghĩa tên miền 6](#_Toc70578228)

[1.1.2. Các thành phần chính của DNS 6](#_Toc70578229)

[1.2. Tổng quan về DNSSEC 10](#_Toc70578230)

[1.2.1. DNSSEC là gì? 10](#_Toc70578231)

[1.2.2. Giới thiệu về DNSSEC 10](#_Toc70578232)

[1.3. Kết luận 12](#_Toc70578233)

[CHƯƠNG II: NGHIÊN CỨU VỀ DNSSEC 13](#_Toc70578234)

[2.1. Mô hình triển khai DNSSEC 13](#_Toc70578235)

[2.2. Các bản ghi tài nguyên DNSSEC 14](#_Toc70578236)

[2.2.1. Các bản ghi DNSKEY trong một Zone 14](#_Toc70578237)

[2.2.2. Các bản ghi RRSIG trong một Zone 14](#_Toc70578238)

[2.2.3. Bản ghi ký chuyển giao (DS) trong một Zone 15](#_Toc70578239)

[2.2.4. Các bản ghi NSEC trong một Zone 16](#_Toc70578240)

[2.2.5. Bản ghi NSEC3 16](#_Toc70578241)

[2.3. Các phần mở rộng trong DNSSEC 19](#_Toc70578242)

[2.3.1. Các máy chủ tên miền có thẩm quyền 20](#_Toc70578243)

[2.3.2. Máy chủ tên miền đệ quy (Recursive Name Server) 28](#_Toc70578244)

[2.3.3. Bộ phân giải 29](#_Toc70578245)

[2.3.4. Hỗ trợ xác thực DNS 35](#_Toc70578246)

[2.4. Kết luận 43](#_Toc70578247)

[CHƯƠNG 3: ỨNG DỤNG DNSSEC TRONG ĐẢM BẢO AN TOÀN HỆ THỐNG TÊN MIỀN (DNS) 45](#_Toc70578248)

[3.1. Các phương thức tấn công mạng phổ biến 45](#_Toc70578249)

[3.1.1. DNS spoofing (DNS cache poisoning) 45](#_Toc70578250)

[3.1.2. Tấn công khuếch đại dữ liệu DNS (Amplification attack) 46](#_Toc70578251)

[3.1.3. Giả mạo máy chủ DNS (Main in the middle) 46](#_Toc70578252)

[3.2. Kịch bản tấn công DNS 47](#_Toc70578253)

[3.3. Giải pháp DNSSEC đối với kịch bản tấn công DNS 68](#_Toc70578254)

[3.4. Kết luận 75](#_Toc70578255)

[KẾT LUẬN 76](#_Toc70578256)

# LỜI NÓI ĐẦU

Hệ thống máy chủ tên miền DNS (Domain Name System) 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.

Trước tình hình phát triển Internet, thương mại điện tử, chính phủ điện tử mạnh mẽ như hiện nay và an ninh mạng có nhiều biến động phức tạp, tiềm ẩn nhiều nguy cơ về an toàn, an ninh và lộ trình, xu thế triển khai DNSSEC trên thế giới thì việc triển khai DNSSEC cho hệ thống máy chủ tên miền (DNS) “.VN” tại Việt Nam là rất cần thiết. Vì vậy, VNNIC đã xây dựng và trình Bộ trưởng Bộ TT&TT ban hành Đề án Triển khai tiêu chuẩn DNSSEC cho hệ thống máy chủ tên miền (DNS) “.VN”. Theo đó, tiêu chuẩn DNSSEC được triển khai áp dụng thống nhất trên hệ thống DNS quốc gia “.VN”, hệ thống DNS của các doanh nghiệp cung cấp dịch vụ Internet (ISP), các nhà đăng ký tên miền “.VN”, các đơn vị cung cấp dịch vụ DNS Hosting và hệ thống DNS của các cơ quan Đảng, Nhà nước.

DNSSEC là phần bảo mật mở rộng trong DNS, được ứng dụng để hỗ trợ cho DNS bảo vệ chống lại các nguy cơ giả mạo làm sai lệch nguồn gốc dữ liệu, DNSSEC cung cấp một cơ chế xác thực giữa các máy chủ DNS với nhau để thiết lập việc xác thực toàn vẹn dữ liệu. Nhận thấy sự cần thiết đó cùng với niềm yêu thích nên em đã lựa chọn nghiên cứu đề tài: “**giới thiệu giao thức thức DNS security”** bao gồm 3 nội dung chính:

* Chương 1: Giới thiệu chung về DNSSEC.
* Chương 2: Nghiên cứu về DNSSEC.
* Chương 3: Ứng dụng DNSSEC trong đảm bảo an toàn hệ thống tên miền

(DNS).

Tuy nhiên, do thời gian có hạn và sự hiểu biết của nhóm em còn nhiều hạn chế, nên không thể tránh được những sai sót. Em rất mong sẽ nhận được sự chỉ bảo của các thầy và các bạn để nhóm em có thể hoàn thiện tốt hơn đề tài của mình.

# CHƯƠNG 1: GIỚI THIỆU CHUNG VỀ DNSSEC

## 1.1. Hệ thống tên miền (DNS – Domain name system)

### **1.1.1. Định nghĩa tên miền**

Hệ thống tên miền bao gồm một loạt các cơ sở dữ liệu chứa địa chỉ IP và các tên miền tương ứng của nó. Mỗi tên miền tương ứng với một địa chỉ bằng số cụ thể. Hệ thống tên miền trên mạng Internet có nhiệm vụ chuyển đổi tên miền sang địa chỉ IP và ngược lại từ địa chỉ IP sang tên miền.

DNS (Domain Name System) là một hệ cơ sở dữ liệu phân tán dùng để ánh xạ giữa các tên miền và các địa chỉ IP. DNS đưa ra một phương thức đặc biệt để duy trì và liên kết các ánh xạ này trong một thể thống nhất.

Trong phạm vi lớn hơn, các máy tính kết nối với Internet sử dụng DNS để tạo địa chỉ liên kết dạng URL (Universal Resource Locators). Theo phương thức này, mỗi máy tính sẽ không cần sử dụng địa chỉ IP cho kết nối mà chỉ cần sử dụng tên miền (domain name) để truy vấn đến kết nối đó.

### **1.1.2. Các thành phần chính của DNS**

Theo đó, khi máy chủ DNS nhận được yêu cầu phân giải địa chỉ từ Resolver, nó sẽ tra cứu bộ đệm (cache) và trả về địa chỉ IP tương ứng với tên miền mà Resolver yêu cầu. Tuy nhiên, nếu không tìm thấy trong bộ đệm, máy chủ DNS sẽ chuyển yêu cầu phân giải tới một máy chủ DNS khác.

Diagram

Description automatically generated

Cấu trúc của DNS là cơ sở dữ liệu dạng cây thư mục, bao gồm từ Top Level Domain (TLDs), Second Level Domain (SLDs), Sub Domain (Host).

DNS có 3 zone chính: Primary zone, Secondary zone và Stub zone. Dữ liệu của các zone được lưu trong một file gọi là zone file. Trong zone file chứa dữ liệu DNS, được thể hiện qua các record như SOA, A, CNAME, MX, NS, SRV.

Hình trên các tên miền iTLD và usTLD thực chất thuộc nhóm gTLD (việc phân tách ra chỉ có ý nghĩa lịch sử). Tên miền cấp cao dùng chung hiện nay được tổ chức quốc tế ICANN (Internet Coroperation for Assigned Names and Numbers) quản lý.

* **Cấu trúc hệ thống tên miền quốc gia .VN:**

Tại Việt Nam, tên miền cấp quốc gia được ICANN phân bổ là ".VN" và nằm trong nhóm tên miền cấp cao quốc gia –ccTLD. Cấu trúc tên miền quốc gia Việt Nam ".VN" được quy định trong Thông tư số 09/2008/TT-BTTTT ngày 24/12/2008 của Bộ Thông tin và Truyền thông :

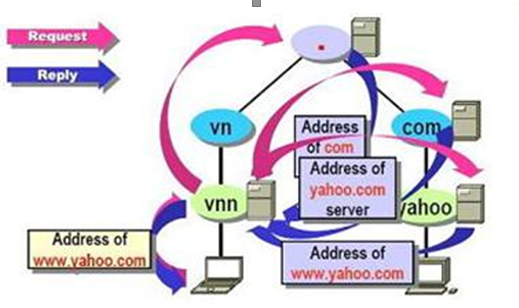
* 1. Tên miền “.VN” là tên miền quốc gia cấp cao nhất dành cho Việt Nam. Các tên miền cấp dưới “.VN” đều có giá trị sử dụng như nhau để định danh địa chỉ Internet cho các máy chủ đăng ký tại Việt Nam.
  2. Tên miền cấp 2 là tên miền dưới “.VN” bao gồm tên miền cấp 2 không phân theo lĩnh vực và tên miền cấp 2 dùng chung (gTLD) phân theo lĩnh vực như sau:
* COM.VN: Dành cho tổ chức, cá nhân hoạt động thương mại.
* BIZ.VN: Dành cho các tổ chức, cá nhân hoạt động kinh doanh, tương đương với tên miền COM.VN.
* EDU.VN: Dành cho các tổ chức, cá nhân hoạt động trong lĩnh vực giáo dục, đào tạo.
* GOV.VN: Dành cho các cơ quan, tổ chức nhà nước ở trung ương và địa phương.
* NET.VN: Dành cho các tổ chức, cá nhân hoạt động trong lĩnh vực thiết lập và cung cấp các dịch vụ trên mạng.
* ORG.VN: Dành cho các tổ chức hoạt động trong lĩnh vực chính trị, văn hoá, xã hội.
* INT.VN: Dành cho các tổ chức quốc tế tại Việt Nam.
* AC.VN: Dành cho các tổ chức, cá nhân hoạt động trong lĩnh vực nghiên cứu.
* PRO.VN: Dành cho các tổ chức, cá nhân hoạt động trong những lĩnh vực có tính chuyên ngành cao.
* INFO.VN: Dành cho các tổ chức, cá nhân hoạt động trong lĩnh vực sản xuất, phân phối, cung cấp thông tin. tế.
* HEALTH.VN: Dành cho các tổ chức, cá nhân hoạt động trong lĩnh vực dược, y
* NAME.VN: Dành cho tên riêng của cá nhân tham gia hoạt động Internet.
* Những tên miền khác do Bô thông tin và Truyền thông quy định.
  1. Các tên miền cấp 2 theo địa giới hành chính là tên miền Internet được đặt theo tên các tỉnh, thành phố trực thuộc trung ương. Tên miền cấp 2 theo địa giới hành chính được viết theo tiếng Việt hoặc tiếng Việt không dấu.
  2. Tên miền tiếng Việt
* Tên miền tiếng Việt nằm trong hệ thống tên miền quốc gia Việt Nam “.VN” trong đó các ký tự tạo nên tên miền là các ký tự được quy định trong bảng mã tiếng Việt theo tiêu chuẩn TCVN 6909:2001 và các ký tự nằm trong bảng mã mở rộng của

tiếng Việt theo tiêu chuẩn nói trên.

* Tên miền tiếng Việt gồm có tên miền cấp 2 và tên miền cấp 3 dưới tên miền cấp 2 theo địa giới hành chính viết theo tiếng Việt. Tên miền phải rõ nghĩa trong ngôn ngữ tiếng Việt, không viết tắt toàn bộ tên miền.

Hệ thống tên miền được sắp xếp theo cấu trúc phân cấp. Mức trên cùng được gọi là ROOT và ký hiệu là “.”, Tổ chức quản lý hệ thống tên miền trên thế giới là The Internet Coroperation for Assigned Names and Numbers (ICANN). Tổ chức này quản lý mức cao nhất của hệ thống tên miền (mức ROOT) do đó nó có quyền cấp phát các tên miền dưới mức cao nhất này.

Để hiểu rõ hơn về hoạt động của DNS, xét ví dụ và tham khảo hình vẽ dưới đây:



Giả sử PC A muốn truy cập đến trang web [http://www.yahoo.com](http://www.yahoo.com/) và máy chủ.vnn chưa lưu thông tin về trang web này, các bước truy vấn sẽ diễn ra như sau:

* Đầu tiên PC A gửi một yêu cầu tới máy chủ quản lý tên miền vnn hỏi thông tin

về [http://www.yahoo.com](http://www.yahoo.com/)

* Máy chủ quản lý tên miền .vnn gửi một truy vấn đến máy chủ top level domain. Top level domain lưu trữ thông tin về mọi tên miền trên mạng. Do đó nó sẽ gửi lại cho máy chủ quản lý tên miền vnn địa chỉ IP của máy chủ quản lý miền com (gọi tắt là máy chủ.com).

Khi có địa chỉ IP của máy chủ quản lý tên miền .com thì lập tức máy chủ.vnn hỏi máy chủ.com thông tin về yahoo.com. Máy chủ com quản lý toàn bộ những trang web có domain là .com, chúng gửi thông tin về địa chỉ IP của máy chủ yahoo.com cho máy chủ vnn.

Lúc này,máy chủ.vnn đã có địa chỉ IP của yahoo.com. Nhưng PC A yêu cầu dịch vụ www chứ không phải là dịch vụ ftp hay một dịch vụ nào khác. Do đó máy chủ.vnn tiếp tục truy vấn tới máy chủ yahoo.com để yêu cầu thông tin về máy chủ quản lý dịch vụ www của yahoo.com.

Khi nhận được truy vấn thì máy chủ yahoo.com gửi lại cho máy chủ.vnn địa chỉ IP của máy chủ quản lý [http://www.yahoo.com/.](http://www.yahoo.com/)

Cuối cùng,máy chủ.vnn gửi lại địa chỉ IP của máy chủ quản lý [http://www.yahoo.com.](http://www.yahoo.com/) cho PC A và PC A kết nối trực tiếp đến nó. Và bây giờ thì máy chủ vnn đã có thông tin về [http://www.yahoo.com](http://www.yahoo.com/) cho những lần truy vấn đến sau của các client khác.

Tuy nhiên, vấn đề là Recursive Domain Name System (DNS) tồn tại lỗ hổng có thể bị tấn công khiến hệ thống quá tải, theo báo cáo của CERT Coordination Center tại Carnegie Mellon University (CERT/CC). Phân giải DNS, xử lí truy vấn DNS với sự trợ giúp của máy chủ có thẩm quyền. Nếu máy chủ này không thể xử lí yêu cầu, nó sẽ chuyển sang máy chủ khác có thể thực hiện nhiệm vụ. Vấn đề là một máy chủ độc hại có thể khiến việc phân giải tên miền theo một chuỗi vô hạn các máy chủ, dẫn đến việc dịch vụ bị quá tải (denial-of-service – DoS). “Việc phân giải DNS theo một quá trình vô hạn dẫn đến việc gia tăng bộ nhớ, CPU và khi quá tải sẽ dừng toàn bộ tiến trình. Những ảnh hưởng có thể từ tăng thời gian máy chủ đáp ứng với khách hàng đến dịch vụ hoàn toàn gián đoạn”.

## 1.2. Tổng quan về DNSSEC

### **1.2.1. DNSSEC là gì?**

DNSSEC (Security Extensions Domain Name System) là công nghệ an toàn mở rộng cho hệ thống DNS (Domain Name System). Trong đó, DNSSEC sẽ cung cấp một cơ chế xác thực giữa các máy chủ DNS với nhau và xác thực cho từng vùng dữ liệu để đảm bảo toàn vẹn dữ liệu.

### **1.2.2. Giới thiệu về DNSSEC**

Trước nguy cơ dữ liệu DNS bị giả mạo và bị làm sai lệch trong các tương tác giữa máy chủ DNS với các resolver hoặc máy chủ forwarder. Trong khi giao thức DNS thông thường không có công cụ để xác thực nguồn gốc dữ liệu, thì công nghệ bảo mật mới DNSSEC (DNS Security Extensions) đã được nghiên cứu, triển khai áp dụng để hỗ trợ cho DNS bảo vệ chống lại các nguy cơ giả mạo làm sai lệch nguồn gốc dữ liệu. Mục tiêu là DNSSEC sẽ cung cấp một cơ chế xác thực giữa các máy chủ DNS với nhau để thiết lập việc xác thực toàn vẹn dữ liệu và chống tấn công từ chối tồn tại. DNSSEC được đề cập trong các tiêu chuẩn RFC: 4033, 4034, 4035….

DNSSEC có 3 chức năng/nhiệm vụ chính:

* **Sender Authentication**: Chứng thực dữ liệu cho quá trình gửi đi.
* **Data Integrity**: Bảo vệ toàn vẹn dữ liệu trong quá trình truyền, giúp người

nhận được đảm bảo dữ liệu không bị thay đổi.

* **Authenticated denial of existence**: Ngăn chặn kẻ tấn công phá hoại bằng cáchcho phép một Resolver xác nhận hợp lệ một tên miền cụ thể nào đó không tồn tại mà Client truy vấn.

Để thực hiện các nhiệm vụ trên, ngoài 4 phần tử chính trong hệ thống DNS (Delegation, Zone file management, Zone file distribution, Resolving), DNSSEC sẽ có thêm một số phần tử như Zone File Signing, Verifying, Trust Anchor, Key rollover, DNS Aware, Key Master. Nhờ đó, DNSSEC đưa ra 5 loại bản ghi mới:

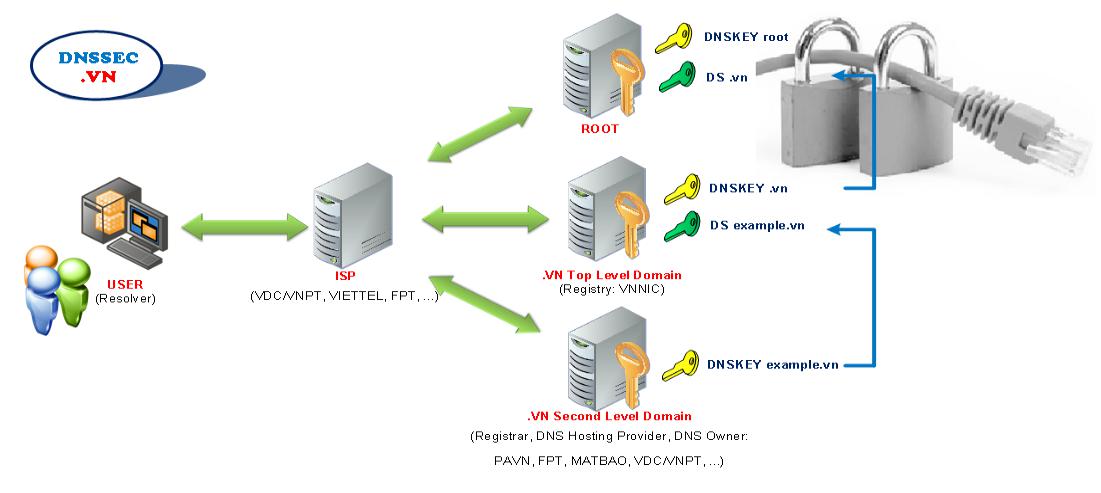
* + **Bản ghi khóa DNS (DNSKEY - DNS Key)**: Sử dụng để chứng thực zone dữ liệu
  + **Bản ghi chữ ký tài nguyên (RRSIG - Resource Record Signature)**: Sử dụng để chứng thực cho các bản ghi tài nguyên trong zone dữ liệu.
  + **Bản ghi ký chuyển giao (DS - Delegation Signer)**: Thiết lập chứng thực giữa các zone dữ liệu, sử dụng trong việc ký xác thực trong quá trình chuyển giao DNS.
  + **Bản ghi bảo mật kế tiếp (NSEC)**: Sử dụng trong quá trình xác thực đối với cácbản ghi có cùng sở hữu tập các bản ghi tài nguyên hoặc bản ghi CNAME. Kết hợp với bản ghi RRSIG để xác thực cho zone dữ liệu.
  + **Bản ghi bảo mật kế tiếp phiên bản 3 (NSEC3)**: Về cơ bản, bản ghi NSEC3 cóchức năng tương tự như bản ghi NSEC trong việc xác thực từ chối sự tồn tại dữ liệu trong zone. Tuy nhiên, trong quá trình sử dụng NSEC thực tế, dữ liệu DNS vẫn có khả năng bị khai thác bởi kỹ thuật tấn công “zone walking”, qua đó cho phép kẻ tấn công liệt kê, thăm dò lấy tất cả các thông tin DNS. Do đó, NSEC3 ra đời sử dụng mã hóa hàm băm nhằm tăng tính bảo mật DNS hơn so với bản ghi NSEC.

Mục tiêu đặt ra là DNSSEC không làm thay đổi tiến trình truyền dữ liệu DNS và quá trình chuyển giao từ các DNS cấp cao xuống các DNS cấp thấp hơn, mặt khác đối với các Resolver cần đáp ứng khả năng hỗ trợ các cơ chế mở rộng này. Một zone

dữ liệu được ký xác thực sẽ chứa đựng một trong các bản ghi RRSIG, DNSKEY, NSEC và DS.

Như vậy bằng cách tổ chức thêm những bản ghi mới và những giao thức đã được chỉnh sửa nhằm chứng thực nguồn gốc và tính toàn vẹn dữ liệu cho hệ thống, với DNSSEC, hệ thống DNS đã được mở rộng thêm các tính năng bảo mật và được tăng cường độ an toàn, tin cậy, khắc phục được những nhược điểm của thiết kế sơ khai ban đầu. Vừa đáp ứng được các yêu cầu thông tin định tuyến về tên miền, giao thức làm việc giữa các máy chủ DNS với nhau, vừa đáp ứng được các yêu cầu bảo mật, tăng cường khả năng dự phòng cho hệ thống.

DNSSEC cung cấp một cơ chế xác thực giữa các máy chủ DNS với nhau (chain of trust) theo cấu trúc hình cây của hệ thống DNS, bắt đầu từ máy chủ ROOT DNS.



Việc xây dựng được chuỗi tin cậy trong DNSSEC là bắt buộc, là cơ sở đảm bảo xác thực nguồn gốc và toàn vẹn dữ liệu trong DNSSEC. Chuỗi tin cậy được thực hiện từng bước, bắt đầu từ hệ thống máy chủ tên miền gốc (DNS ROOT) đến các máy chủ TLD, cho tới các hệ thống DNS cấp dưới. Sau khi được triển khai đầy đủ, việc hacker tấn công hệ thống DNS, chuyển hướng tên miền sẽ bị phát hiện và ngăn chặn.

Từ đó việc truy cập vào các dịch vụ trên tên miền được đảm bảo an toàn, xác thực, các nguy cơ đã trình bày ở trên được giải quyết.

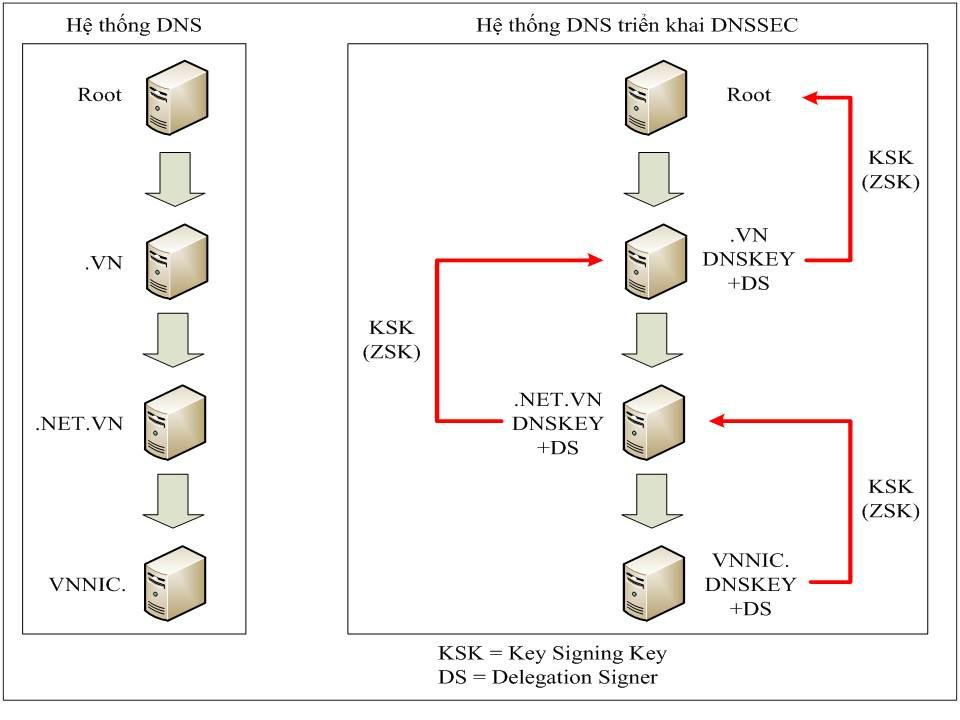
## 1.3. Kết luận

Trong chương này đã giới thiệu tổng quan về Hệ thống tên miền DNS. Bao gồm định nghĩa và các thành phần chính của hệ thống tên miền DNS. Các lỗ hổng trong vấn đề bảo mật của DNS và sự cần thiết trong việc khắc phục những vấn đề đó. DNSSEC - ứng dụng bảo mật tên miền được đưa ra để giải quyết bài toán bảo mật cho DNS. Cụ thể về DNSSEC đã giới thiệu về khái niệm, mục đích chức năng. Tình hình triển khai cũng như các tiêu chuẩn chuẩn hóa của DNSSEC trên thế giới và tại Việt Nam. Nêu ra một số tổ chức tiêu chuẩn trên Thế Giới. Và lộ trình triển khai ở Việt Nam.

Với tính chất đảm bảo an ninh mạng cũng như ưu điểm và khả năng ứng dụng thực tế cao nên việc đưa DNSSEC áp dụng tại Việt Nam là hết sức cần thiết.

# CHƯƠNG II: NGHIÊN CỨU VỀ DNSSEC

## 2.1. Mô hình triển khai DNSSEC

****

Quá trình triển khai DNSSEC bao gồm: Ký chuyển giao tên miền .VN từ DNS Root về máy chủ DNS quốc gia quản lý và ký chuyền giao tên miền từ máy chủ DNS quốc gia cho các đơn vị khác quản lý. Việc triển khai DNSSEC trên hệ thống DNS quốc gia gồm các bước như sau:

Trên máy chủ DNS:

* BƯỚC 1: Tạo cặp khóa riêng và khóa công khai
* BƯỚC 2: Lưu trữ bảo mật khóa riêng
* BƯỚC 3: Phân phối khóa công khai
* BƯỚC 4: Ký zone
* BƯỚC 5: Thay đổi khóa
* BƯỚC 6: Ký lại zone

Trên resolver:

* BƯỚC 7: Cấu hình Trust Anchors
* BƯỚC 8: Thiết lập chuỗi tin cậy và xác thực chữ ký

## 2.2. Các bản ghi tài nguyên DNSSEC

Trong DNSSEC đưa ra khác niệm các Signed Zone. Signed Zone có khóa công khai DNS (DNSKEY), chữ ký bản ghi tài nguyên (RRSIG), bảo mật kế tiếp (NSEC) và tùy chọn các bản ghi ký chuyển giao (DS) tùy theo các nguyên tắc được quy định.

### **2.2.1. Các bản ghi DNSKEY trong một Zone**

Để ký một Zone, quản trị Zone đó tạo một hoặc nhiều cặp khóa công khai/ mật và sử dụng (các) khóa mật để ký các tập bản ghi có thẩm quyền trong Zone đó. Đối với mỗi khóa mật được sử dụng để tạo các bản ghi RRSIG trong một Zone, Zone này nên có một bản ghi DNSKEY của Zone chứa khóa công khai tương ứng. Bản ghi DNSKEY chứa khóa công khai này của Zone phải có bit khóa công khai của Zone thuộc trường Flags RDATA được thiết lập. Các khóa công khai liên kết với các hoạt động DNS khác có thể được chứa trong các bản ghi DNSKEY không được xác định là các khóa công khai của Zone thì không được sử dụng để kiểm tra các RRSIG.

Khi quản trị Zone này định một Signed Zone có thể được sử dụng ngoài chức năng một Island of Security thì Zone apex phải có ít nhất một bản ghi DNSKEY được hoạt động như một điểm truy nhập bảo mật vào Zone này. Do đó, điểm truy nhập bảo mật này có thể được sử dụng làm đích của một chuyển giao bảo mật thông qua một bản ghi DS tương ứng trong Zone.

Bản ghi chứng thực DNSKEY cho Zone phải có bit Zone Key của trường dữ liệu cờ đặt giá trị là 1. Nếu quản trị zone có ý định ký một zone để chứng thực thì zone chính phải chứa đựng ít nhất một bản ghi DNSKEY để hoạt động như một điểm bảo mật ở trong zone. Điểm bảo mật được dùng cùng với bản ghi DS tương ứng ở zone cha trong hoạt động chuyển giao DNS.

### **2.2.2. Các bản ghi RRSIG trong một Zone**

Đối với mỗi tập bản ghi có thẩm quyền trong một Signed Zone, phải có ít nhất một bản ghi RRSIG đáp ứng các yêu cầu sau:

* Tên sở hữu RRSIG này giống tên sở hữu tập bản ghi này.
* Lớp RRSIG này giống lớp của tập bản ghi này.
* Trường RRSIG Type Covered giống loại của tập bản ghi này.
* Trường RRSIG Original TTL giống TTL của tập bản ghi này.
* TTL của bản ghi RRSIG này giống TTL của tập bản ghi này.
* Trường RRSIG Labels giống số nhãn trong tên sở hữu của tập bản ghi này, không tính nhãn null root và nhãn phía trái ngoài cùng khi nó là một ký tự đại diện.
* Trường Name của RRSIG Signer giống tên của zone chứa tập bản ghi này.
* Các trường RRSIG Algorithm, Name của Signer và Key Tag giống bản ghi DNSKEY chứa khóa công khai của zone tại zone apex.

Tập bản ghi có thể có nhiều bản ghi RRSIG liên kết với nó. Vì bản ghi RRSIG liên kết chặt với các tập bản ghi mà các chữ ký được các bản ghi RRSIG chứa không giống tất cả các loại bản ghi DNS khác, không tạo nên các tập bản ghi. Cụ thể là các giá trị TTL trong các bản ghi RRSIG có tên sở hữu chung không tuân theo các nguyên tắc của tập bản ghi.

Một bản ghi RRSIG không được tự ký vì việc ký một bản ghi RRSIG sẽ không có giá trị và sẽ tạo một vòng lặp không xác định trong quá trình ký.

Tập bản ghi NS xuất hiện tại tên của zone apex phải được ký nhưng các tập bản ghi NS xuất hiện tại các điểm chuyển giao (tức là các tập bản ghi NS trong zone cha mà ủy quyền tên này cho các máy chủ tên miền của zone con) không được ký. Các tập bản ghi địa chỉ liên kết được liên kết với những ủy quyền không được ký.

Phải có một RRSIG đối với mỗi tập bản ghi sử dụng ít nhất một DNSKEY của mỗi thuật toán trong tập bản ghi DNSKEY của zone apex. Tập bản ghi DNS của zone apex này phải được tự ký bằng mỗi thuật toán xuất hiện trong tập bản ghi DS được đặt ở phía cha ủy quyền (nếu có).

### **2.2.3. Bản ghi ký chuyển giao (DS) trong một Zone**

Bản ghi DS – Delegation Signer thiết lập chứng thực giữa những zone DNS. Một bản ghi DS được biểu diễn cho bản ghi chuyển giao khi vùng con được ký. Bản ghi DS kết hợp với bản ghi RRSIG để chứng thực cho zone được chuyển giao tại máy chủ tên miền cha. Bản ghi DS được khai báo trước, và bản ghi RRSIG khai báo sau giống như khai báo để xác thực cho một bản ghi tài nguyên thông thường.

Trường TTL của tập bản ghi DS phải ứng với trường TTL của tập bản ghi NS chuyển giao (có nghĩa là tập bản ghi NS trong cùng vùng chứa tập bản ghi DS). Việc xây dựng một bản ghi DS đòi hỏi phải có hiểu biết của bản ghi DNSKEY tương ứng trong vùng con để đưa ra được các giao tiếp giữa vùng con và vùng cha.

### **2.2.4. Các bản ghi NSEC trong một Zone**

Mỗi tên sở hữu trong zone có dữ liệu có thẩm quyền hoặc một tập bản ghi NS của điểm chuyển giao phải có một bản ghi tài nguyên NSEC. Giá trị TTL đối với bất kỳ bản ghi NSEC nên giống trường giá trị TTL tối thiểu trong bản ghi SOA của zone này.

Một bản ghi NSEC (và tập bản ghi RRSIG được liên kết với nó) không được là tập bản ghi duy nhất ở tên sở hữu cụ thể bất kỳ nào. Do đó, quá trình ký này không được tạo các bản ghi NSEC hoặc RRSIG đối với các nút tên sở hữu chưa là tên sở hữu của bất kỳ tập bản ghi trước khi zone này được ký. Các lý do chính của điều này là cần sự nhất quán không gian tên giữa các phiên bản được ký và chưa ký của cùng một zone và giảm nguy cơ mất nhất quán đặc trưng trong các máy chủ tên miền đệ quy không có bảo mật.

Ánh xạ loại của mỗi bản ghi NSEC trong một Signed Zone phải chỉ ra sự có mặt của cả chính bản ghi NSEC này và bản ghi RRSIG tương ứng.

Sự khác nhau giữa bộ các tên sở hữu có yêu cầu các bản ghi RRSIG và bộ các tên sở hữu có yêu cầu các bản ghi NSEC là tinh vi và đáng nêu rõ. Các bản ghi RRSIG có ở các tên sở hữu của tất cả các tập bản ghi có thẩm quyền. Các bản ghi NSEC có ở các tên sở hữu của tất cả các tên mà Signed Zone có thẩm quyền đối với chúng và ở các tên sở hữu của những ủy quyền từ Signed Zone sang zone con của nó. Các bản ghi NSEC hoặc RRSIG không có (trong zone cha) ở các tên sở hữu của các tập bản ghi địa chỉ liên kết. Tuy nhiên, chú ý rằng sự khác biệt này chỉ là phần dễ thấy nhất trong quá trình ký zone vì các tập bản ghi NSEC là dữ liệu có thẩm quyền và do đó được ký. Do đó, bất kỳ tên sở hữu nào có một tập bản ghi NSEC cũng sẽ có các bản ghi RRSIG trong Signed Zone.

Việc ánh xạ đối với bản ghi NSEC ở điểm chuyển giao yêu cầu sự quan tâm đặc biệt. Các bit tương ứng tập bản ghi NS ủy quyền và bất kỳ các tập bản ghi mà zone cha có dữ liệu có thẩm quyền đối với chúng phải được thiết lập; các bit tương ứng bất kỳ tập bản ghi không là NS mà phía cha không có thẩm quyền đối với chúng phải xóa.

### **2.2.5. Bản ghi NSEC3**

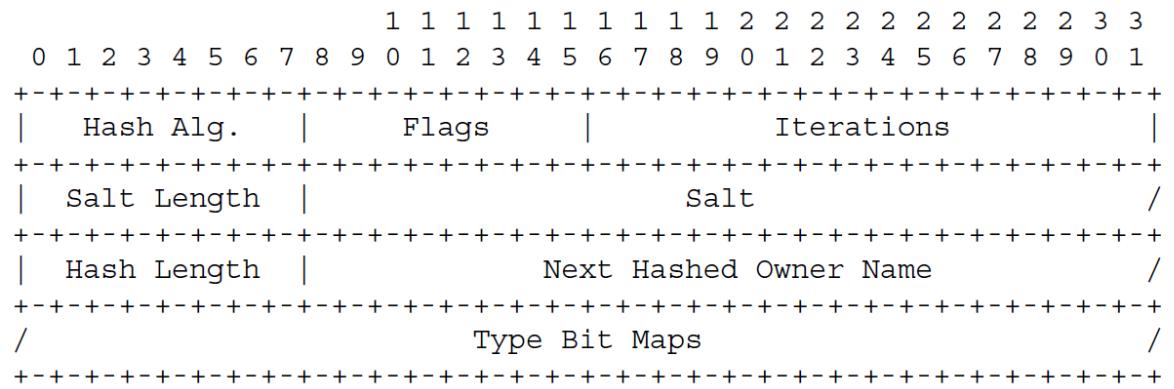
Có 2 vấn đề khi sử dụng bản ghi NSEC trong DNSSEC:

* Vấn đề thứ nhất: dữ liệu có thể bị tấn công “zone walking”. Có thể thấy theo ví dụ trên, các bản ghi NSEC trỏ từ một tên miền này đến một tên miền khác: tên miền “example.org” trỏ tới tên miền “a.example.org”, rồi từ “a.example.org” trỏ tiếp đến “d.example.org” và cuối cùng trỏ trở lại “example.org”, tạo thành một chuỗi bản ghi NSEC. Do đó, kẻ tấn công có thể tái xây dựng lại cấu trúc zone “example.org” nhằm thăm dò dữ liệu và ngăn việc trao đổi dữ liệu trong zone.
* Vấn đề thứ hai: khi phát triển zone có chuyển giao trung tâm kích cỡ lớn trong DNSSEC, tất cả tên miền trong zone được gán một bản ghi NSEC kèm bản ghi ký RRSIG. Điều đó làm tăng kích thước zone (khi ký). Có nghĩa là các nhà khai thác phát triển DNSSEC sẽ đối mặt với tăng chi phí đầu tư.

Để giải quyết các vấn đề này, NSEC3 được giới thiệu và đề xuất nhằm giải quyết các vấn đề mà NSEC gặp phải nhưng đồng thời độ phức tạp sử dụng cũng cao hơn. NSEC3 ra đời không phải để thay thế NSEC mà cùng tồn tại trong DNSSEC. Tuy nhiên, trong cùng một zone, không thể sử dụng đồng thời cả NSEC và NSEC3. Có nghĩa là, có hai cách thức khác nhau để thực hiện xác thực từ chối sự tồn tại: NSEC và NSEC3.

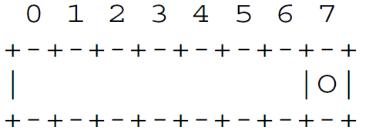
NSEC3 sử dụng mã hóa hàm băm tất cả tên miền. Do đó, chuỗi bản ghi NSEC3 được sắp xếp theo thứ tự mã băm, thay vì thứ tự chính tắc. Có thể thấy, ở ví dụ trên, theo thứ tự chính tắc, tên miền kế tiếp của “example.org” là “a.example.org”. Tuy nhiên, vì tất cả tên miền khi chuyển đổi sang NSEC3 đều được mã hóa băm nên tên miền kế tiếp của “example.org” không phải là “a.example.org” nữa mà là “d.example.org”. Vì vậy, tấn công “zone walking” khó thực hiện liệt kê thăm dò dữ liệu.

Về cấu trúc bản ghi NSEC3, định dạng RDATA của bản ghi tài nguyên NSEC3 được chia thành các trường độc lập và các trường tương ứng với các trường của tên miền.



***Trường Hash Algorithm***: Định nghĩa thuật toán mã hóa băm được sử dụng đểtạo nên giá trị mã băm và có giá trị là một octet đơn nhất.

***Trường Flags***: Bao gồm 8 cờ 1 bit có thể được sử dụng để chỉ báo tiến trình khácnhau. Tất cả cờ không được định nghĩa phải bằng 0 và có giá trị là một octet đơn nhất. Cờ Opt-Out là bit có trọng số thấp nhất, có định dạng như dưới đây:



***Trường Iteration***: Xác định số lần lặp bổ sung cho số lần lặp mà hàm băm đãthực hiện. Số lần lặp lớn hơn làm tăng tính bền vững của giá trị mã hóa băm chống lại các cuộc tấn công dạng từ điển nhưng mất nhiều thời gian tính toán hơn ở cả máy chủ và Resolver. Trường Iterations được biểu diễn bằng một số nguyên không dấu 16-bit, với bit đầu có trọng số cao nhất.

***Trường Salt Length***: Được biểu diễn bằng một octet không dấu và định nghĩa độdài của trường Salt theo các octet, có dải giá trị từ 0 đến 255. Nếu giá trị bằng 0, thì trường Salt sau đây bị bỏ qua.

***Trường Salt (nếu có)***: Được mã hóa bằng một chuỗi octet nhị phân và được bổsung vào tên miền gốc trước khi mã hóa băm để ngăn chặn các cuộc tấn công dạng từ điển được thực hiện.

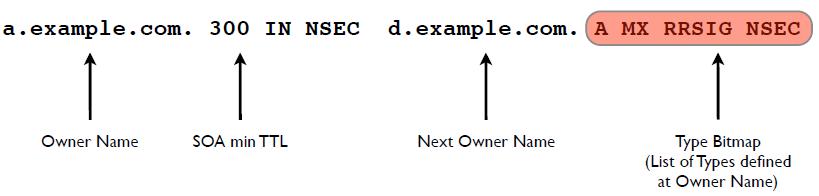
***Trường Hash Length***: Được biểu diễn bằng một octet không dấu và định nghĩađộ dài của trường Next Hashed Owner Name, có dải giá trị từ 1 đến 255 octet.

***Trường Next Hashed Owner Name***: Không được mã hóa base32, khác với tênmiền của bản ghi tài nguyên NSEC3. Đây là giá trị mã hóa băm nhị phân không sửa đổi. Không bao gồm tên của zone chứa nó. Độ dài của trường này được trường Hash Length đứng trước quyết định.

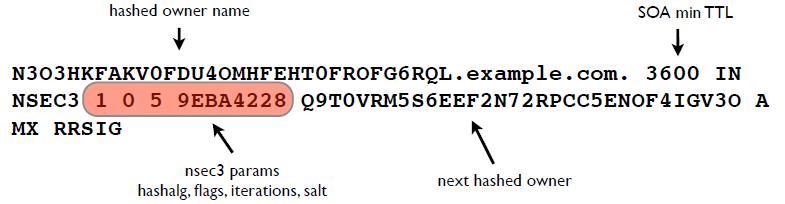
***Trường Type Bit Maps***: Định danh các loại bản ghi tài nguyên hiện hữu trong tênmiền gốc của bản ghi tài nguyên NSEC3.

Để đối chiếu cấu trúc giữa NSEC và NSEC3, ta có 1 ví dụ khác như sau:

Một bản tin khi sử dụng bản ghi tài nguyên NSEC với cấu trúc như sau:



Trong khi, bản tin sử dụng bản ghi tài nguyên NSEC3 tương ứng với tên miền được mã hóa băm (mã hóa base32 với mã hex mở rộng):



Có thể thấy, tên miền và tên miền kế tiếp được mã hóa hàm băm khi sử dụng bản ghi NSEC3. Ngoài ra, bản tin chứa bản ghi tài nguyên NSEC3 còn bổ sung thêm bản tài nguyên NSEC3PARAM, gồm các trường HashAlg, Flags, Iteration và Salt.

Có một lưu ý, trong DNSSEC, việc sử dụng NSEC3 không phải lúc nào cũng mang lại hiệu quả. Đối với các zone có cấu trúc mức cao như các zone ip6.arpa hay in-addr.arpa, vẫn có thể dễ dàng bị tấn công zone walking thăm dò dù sử dụng bản ghi NSEC3 do cấu trúc xây dựng của zone. Ngoài ra, với các tên miền nhỏ, các zone ít quan trọng cũng có thể dễ dàng bị suy đoán ra. Trong các trường hợp như vậy, bản ghi NSEC3 không thể ngăn chặn tấn công zone walking mà còn khiến việc tính toán mất nhiều thời gian hơn giữa các máy chủ có thẩm quyền và các thành phần xác minh tính hợp lệ.

## 2.3. Các phần mở rộng trong DNSSEC

Security-Aware Name Server phải hỗ trợ EDNS0 phần mở rộng kích cỡ bản tin phải hỗ trợ kích cỡ bản tin tối thiểu 1220 octet và nên hỗ trợ kích cỡ bản tin 4000 octet. Vì các gói tin IPv6 chỉ có thể được máy tính chủ nguồn phân đoạn, Security-Aware Name Server nên thực hiện các bước để đảm bảo rằng các gói thông tin UDP nó truyền qua IPv6 được phân đoạn ở mức MTU IPv6 tối thiểu nếu cần trừ phi biết MTU của tuyến.

Một Security-Aware Name Server nhận một truy vấn DNS không chứa EDNS OPT giả - bản ghi tài nguyên hoặc có bit DO trống phải đáp ứng các bản ghi tài nguyên RRSIG, DNSKEY và NSEC như đáp ứng bất kỳ tập bản ghi tài nguyên khác và không được thực hiện bất kỳ hành động bổ sung được trình bày dưới đây. Vì loại bản ghi tài nguyên DS có thuộc tính khác thường là chỉ xuất hiện trong zone cha ở các điểm chuyển giao, các bản ghi tài nguyên DS luôn luôn yêu cầu một hành động đặc biệt nào đó.

Các Security-Aware Name Server nhận các truy vấn rõ ràng về các loại bản ghi tài nguyên bảo mật phù hợp nội dung của nhiều hơn một zone mà nó phục vụ (ví dụ các bản ghi tài nguyên NSEC và RRSIG ở trên và dưới điểm chuyển giao nơi máy chủ này có thẩm quyền đối với cả hai zone) nên hành xử nhất quán. Máy chủ tên miền này có thể trả về một trong các nội dung sau miễn là trả lời này luôn nhất quán đối với mỗi truy vấn đến máy chủ tên miền này:

* Các tập bản ghi tài nguyên trên điểm chuyển giao. Các tập bản ghi tài nguyên dưới điểm chuyển giao
* Cả hai tập bản ghi tài nguyên trên và dưới điểm chuyển giao. Phần trả lời trống (không có bản ghi tài nguyên).

DNSSEC phân bố hai bit mới trong phần mào đầu bản tin DNS: bit CD (Checking Disabled) và bit AD (Authentic Data). Bit CD được các Resolver điều khiển; một Security-Aware Name Server phải sao chép bit CD từ một truy vấn thành một trả lời tương ứng. Bit AD được các máy chủ tên miền điều khiển; Security-Aware Name Server phải bỏ qua việc thiết lập bit AD trong các truy vấn. Security-Aware Name Server đồng bộ các bản ghi tài nguyên CNAME từ các bản ghi tài nguyên DNAME không nên tạo các chữ ký đối với các bản ghi tài nguyên CNAME được đồng bộ này.

### **2.3.1. Các máy chủ tên miền có thẩm quyền**

Dựa vào việc nhận một truy vấn liên quan có bit DO EDNS OPT giả - bản ghi tài nguyên được thiết lập, máy chủ tên miền có thẩm quyền có bảo mật đối với một Signed Zone phải chứa các bản ghi tài nguyên RRSIG, NSEC và DS bổ sung tuân theo các nguyên tắc sau:

* Các bản ghi tài nguyên RRSIG có thể được sử dụng để xác thực một trả lời phải được chứa trong trả lời này.
* Các bản ghi tài nguyên NSEC có thể được sử dụng để cung cấp xác nhận từ chối sự tồn tại phải được chứa trong trả lời này.
* Tập bản ghi tài nguyên DS hoặc một bản ghi tài nguyên NSEC chỉ ra rằng không có bản ghi tài nguyên DS nào tồn tại phải được chứa trong các tham chiếu một cách tự động

Các nguyên tắc này chỉ áp dụng cho các trả lời trong đó các cú pháp truyền thông tin về sự có hoặc không có các bản ghi tài nguyên. Do đó, các nguyên tắc này không đưa ra các trả lời giống như “Không được thực hiện” đối với RCODE hay “Bị từ chối” đối với RCODE 5.

DNSSEC không thay đổi giao thức DNS zone transfer.

* **Các bản ghi tài nguyên RRSIG trong một hồi đáp**

Khi trả lời một truy vấn có bit DO được thiết lập, máy chủ tên miền có thẩm quyền có bảo mật nên cố gắng gửi các bản ghi tài nguyên RRSIG mà Security-Aware Resolver có thể sử dụng để xác thực các tập bản ghi tài nguyên này trong trả lời này. Một máy chủ tên miền nên thực hiện mọi cố gắng để giữ tập bản ghi tài nguyên này và (các) RRSIG liên kết của nó trong một trả lời. Việc chứa các bản ghi tài nguyên RRSIG trong một trả lời tuân theo các nguyên tắc sau:

Khi đặt một tập bản ghi tài nguyên được ký trong phần trả lời, máy chủ tên miền này cũng phải đặt các bản ghi tài nguyên RRSIG của nó trong phần trả lời đó. Các bản ghi tài nguyên RRSIG này có mức ưu tiên bao hàm cao hơn bất kỳ các tập bản ghi tài nguyên khác có thể phải được bao hàm. Khi không gian không cho phép bao hàm các bản ghi tài nguyên RRSIG này, máy chủ tên miền này phải thiết lập bit TC.

Khi đặt một tập bản ghi tài nguyên được ký trong phần thẩm quyền, máy chủ tên miền cũng phải đặt các bản ghi tài nguyên RRSIG của nó trong phần thẩm quyền. các bản ghi tài nguyên RRSIG này có mức ưu tiên bao hàm cao hơn bất kỳ các tập bản ghi tài nguyên khác có thể phải được bao hàm. Khi không gian không cho phép bao hành các bản ghi tài nguyên RRSIG này, máy chủ tên miền phải thiết lập bit TC.

Khi đặt một tập bản ghi tài nguyên được ký trong phần bổ sung, máy chủ tên miền cũng phải đặt các bản ghi tài nguyên RRSIG của nó trong phần bổ sung. Khi không gian không cho phép bao hàm cả tập bản ghi tài nguyên này và các bản ghi tài nguyên RRSIG liên kết của nó, máy chủ tên miền có thể giữ lại tập bản ghi tài nguyên này và thả các bản ghi tài nguyên RRSIG. Khi điều này xảy ra, máy chủ tên miền không được thiết lập bit TC vì các bản ghi tài nguyên RRSIG đã không phù hợp.

* **Các bản ghi tài nguyên DNSKEY trong một hồi đáp**

Khi trả lời một truy vấn có bit DO được thiết lập và yêu cầu các bản ghi tài nguyên SOA hoặc NS ở zone apex được ký, máy chủ tên miền có thẩm quyền có bảo mật đối với zone đó có thể trả về tập bản ghi tài nguyên DNSKEY của zone apex này trong phần bổ sung. Trong trường hợp này, tập bản ghi tài nguyên DNSKEY và các bản ghi tài nguyên RRSIG liên kết có mức ưu tiên thấp hơn bất kỳ thông tin khác được đặt trong phần bổ sung. Máy chủ tên miền không nên bao hàm tập bản ghi tài nguyên DNSKEY này trừ khi có đủ không gian trong bản tin trả lời dành cho cả tập bản ghi tài nguyên DNSKEY và (các) bản ghi tài nguyên RRSIG liên kết của nó. Khi không có đủ không gian để bao hàm DNSKEY và các bản ghi tài nguyên RRSIG này, máy chủ tên miền phải loại bỏ chúng và không được thiết lập bit TC vì các bản ghi tài nguyên này đã không phù hợp.

* **Các bản ghi tài nguyên NSEC trong một hồi đáp**

Khi trả lời một truy vấn có bit DO được thiết lập , máy chủ tên miền có thẩm quyền có bảo mật đối với zone đó phải bao hàm các bản ghi tài nguyên NSEC trong một trong các trường hợp sau:

* Không có dữ liệu: Zone chứa các tập bản ghi tài nguyên phù hợp hoàn toàn <SNAME, SCLASS> nhưng không chứa bất kỳ tập bản ghi tài nguyên phù hợp hoàn toàn <SNAME, SCLASS, STYPE>
* Lỗi tên miền: Zone không chứa bất kỳ tập bản ghi tài nguyên phù hợp <SNAME, SCLASS> một cách hoàn toàn hoặc thông qua phần mở rộng tên miền ký tự đại diện
* Trả lời ký tự đại diện: Zone không chứa bất kỳ tập bản ghi tài nguyên phù hợp hoàn toàn <SNAME, SCLASS> nhưng chứa một tập bản ghi tài nguyên phù hợp <SNAME, SCLASS, STYPE> thông qua phần mở rộng tên miền ký tự đại diện.
* Không có dữ liệu ký tự đại diện: Zone không chứa bất kỳ tập bản ghi tài nguyên phù hợp hoàn toàn <SNAME, SCLASS> và chứa một hoặc nhiều tập bản ghi tài nguyên phù hợp <SNAME, SCLASS> thông qua phần mở rộng tên miền ký tự đại diện nhưng không chứa bất kỳ tập bản ghi tài nguyên phù hợp <SNAME, SCLASS, STYPE> thông qua phần mở rộng tên miền ký tự đại diện.

Trong mỗi trường hợp này, máy chủ tên miền bao hàm các bản ghi tài nguyên NSEC trong trả lời để chỉ ra rằng sự phù hợp hoàn toàn đối với <SNAME, SCLASS, STYPE> không có trong zone này và rằng trả lời này máy chủ tên miền trả về là đúng với dữ liệu trong zone này.

***Các bản ghi tài nguyên NSEC: Hồi đáp không có dữ liệu***

Khi zone chứa các tập bản ghi tài nguyên phù hợp <SNAME, SCLASS> nhưng không chứa tập bản ghi tài nguyên phù hợp <SNAME, SCLASS, STYPE> thì máy chủ tên miền phải bao hàm bản ghi tài nguyên NSEC dành cho <SNAME, SCLASS> cùng với (các) bản ghi tài nguyên RRSIG liên kết của nó trong phần thẩm quyền của trả lời. Khi không gian không cho phép bao hàm bản ghi tài nguyên NSEC hoặc (các) bản ghi tài nguyên RRSIG liên kết của nó, máy chủ tên miền phải thiết lập bit TC.

Khi tên miền tìm kiếm tồn tại, phần mở rộng tên miền ký tự đại diện không áp dụng đối với truy vấn này và một bản ghi tài nguyên NSEC được ký duy nhất đủ để chỉ ra rằng loại bản ghi tài nguyên được yêu cầu không tồn tại.

***Các bản ghi tài nguyên NSEC: Hồi đáp lỗi tên miền***

Khi zone không chứa bất kỳ tập bản ghi tài nguyên phù hợp <SNAME, SCLASS> hoàn toàn hoặc thông qua phần mở rộng tên miền ký tự đại diện thì máy chủ tên miền phải bao hàm các bản ghi tài nguyên NSEC sau trong phần thẩm quyền cùng với các bản ghi tài nguyên RRSIG liên kết của nó:

* Một bản ghi tài nguyên NSEC chỉ ra rằng không có phù hợp hoàn toàn dành cho <SNAME, SCLASS>.
* Một bản ghi tài nguyên NSEC chỉ ra rằng zone này không chứa các tập bản ghi tài nguyên phù hợp <SNAME, SCLASS> thông qua phần mở rộng tên miền ký tự đại diện.

Trong một số trường hợp, một bản ghi tài nguyên NSEC có thể chỉ ra cả hai điều này. Khi đó, máy chủ tên miền chỉ nên bao hàm bản ghi tài nguyên NSEC này và (các) bản ghi tài nguyên RRSIG của nó trong phần thẩm quyền.

Khi không gian không cho phép bao hàm các bản ghi tài nguyên NSEC và RRSIG này, máy chủ tên miền phải thiết lập bit TC.

Các tên miền chủ của các bản ghi tài nguyên NSEC và RRSIG này không phụ thuộc vào phần mở rộng tên miền ký tự đại diện khi các bản ghi tài nguyên này được bao hàm trong phần thẩm quyền của trả lời.

Dạng trả lời bao hàm các trường hợp trong đó SNAME tương ứng một tên miền trống không kết thúc trong zone đó (một tên miền không là tên miền chủ đối với bất kỳ tập bản ghi tài nguyên nhưng là tên miền cha của một hoặc nhiều tập bản ghi tài nguyên)

***Các bản ghi tài nguyên NSEC: Hồi đáp trả lời ký tự đại diện***

Khi zone này không chứa bất kỳ các tập bản ghi tài nguyên phù hợp hoàn toàn <SNAME, SCLASS> nhưng chứa một tập bản ghi tài nguyên phù hợp <SNAME, SCLASS, STYPE> thông qua phần mở rộng tên miền ký tự đại diện, máy chủ tên miền này phải chứa trả lời có phần mở rộng ký tự đại diện và các bản ghi tài nguyên RRSIG có phần mở rộng ký tự đại diện tương ứng trong phần trả lời và phải chứa trong phần thẩm quyền một bản ghi tài nguyên NSEC và (các) bản ghi tài nguyên RRSIG tương ứng chỉ ra rằng zone này không chứa một phù hợp gần với <SNAME, SCLASS>. Khi không gian không cho phép bao hàm trả lời, các bản ghi tài nguyên NSEC và RRSIG, máy chủ tên miền này phải thiết lập bit TC.

***Các bản ghi tài nguyên NSEC: Hồi đáp không có dữ liệu ký tự đại diện***

Trường hợp này là sự kết hợp của các trường hợp trước. Zone này không chứa sự phù hợp hoàn toàn đối với <SNAME, SCLASS> và mặc dù zone này chứa các tập bản ghi tài nguyên phù hợp <SNAME, SCLASS> thông qua phần mở rộng ký tự đại diện, không có tập bản ghi tài nguyên nào phù hợp STYPE. Máy chủ tên miền phải bao hàm các bản ghi tài nguyên NSEC sau trong phần thẩm quyền cùng với các bản ghi tài nguyên RRSIG liên kết của chúng:

* Một bản ghi tài nguyên NSEC chỉ ra rằng không có tập bản ghi tài nguyên nào phù hợp STYPE ở tên miền chủ ký tự đại diện mà phù hợp <SNAME, SCLASS> thông qua phần mở rộng ký tự đại diện.
* Một bản ghi tài nguyên NSEC chỉ ra rằng không có tập bản ghi tài nguyên nào trong zone này phù hợp gần với <SNAME, SCLASS>.

Trong một số trường hợp, một bản ghi tài nguyên NSEC đơn có thể chỉ ra cả hai điều này. Khi đó, máy chủ tên miền chỉ nên bao hàm bản ghi tài nguyên NSEC này và (các) bản ghi tài nguyên RRSIG của nó trong phần thẩm quyền.

Tên miền chủ của các bản ghi tài nguyên NSEC và RRSIG này không phụ thuộc vào phần mở rộng tên miền ký tự đại diện khi các bản ghi tài nguyên này được bao hàm trong phần thẩm quyền của trả lời.

Khi không gian không cho phép bao hàm các bản ghi tài nguyên NSEC và RRSIG này, máy chủ tên miền phải thiết lập bit TC.

***Tìm các bản ghi tài nguyên NSEC đúng***

Như được trình bày ở trên, có một số tình huống trong đó máy chủ tên miền có thẩm quyền có bảo mật phải đặt một bản ghi tài nguyên NSEC để chỉ ra rằng không có tập bản ghi tài nguyên nào phù hợp một SNAME cụ thể hiện có. Việc đặt một bản ghi tài nguyên NSEC trong một zone có thẩm quyền như vậy tương đối đơn giản, ít nhất về mặt khái niệm. Phần thảo luận sau giả thiết rằng máy chủ tên miền này có thẩm quyền đối với zone chứa các tập bản ghi tài nguyên không tồn tại phù hợp SNAME. Thuật toán sau được viết để làm rõ dù không hiệu quả.

Để tìm NSEC chỉ ra rằng không có tập bản ghi tài nguyên nào phù hợp tên miền N tồn tại trong zone Z chứa chúng, xây dựng một câu S bao gồm các tên miền chủ của mỗi tập bản ghi tài nguyên trong Z, được sắp xếp theo thứ tự chính tắc (RFC 4034) không có tên miền trùng lặp. Tìm tên miền M đứng ngay trước N trong S khi bất kỳ tập bản ghi tài nguyên có tên miền chủ N tồn tại. M là tên miền chủ của bản ghi tài nguyên NSEC chỉ ra rằng không có tập bản ghi tài nguyên nào tồn tại có tên miền chủ N.

Thuật toán tìm bản ghi tài nguyên NSEC này chỉ ra rằng một tên miền cho trước không được bất kỳ ký tự đại diện có thể áp dụng nào che đậy là tương tự nhưng yêu cầu thêm một bước. Nói một cách chính xác hơn, thuật toàn tìm NSEC chỉ ra rằng không tập bản ghi tài nguyên nào tồn tại có tên miền ký tự đại diện có thể áp dụng là giống thuật toán tìm bản ghi tài nguyên NSEC chỉ ra rằng các tập bản ghi tài nguyên có bất kỳ một tên miền chủ khác không tồn tại. Phần thiếu là phương pháp xác định tên miền của ký tự đại diện có thể áp dụng không tồn tại. Thực tế, điều này là dễ dàng vì máy chủ tên miền có thẩm quyền đã tìm kiếm sự có mặt của tên miền ký tự đại diện này như một phần của bước (1).

* **Các bản ghi tài nguyên DS trong một hồi đáp**

Khi trả lời một truy vấn có bit DO được thiết lập, máy chủ tên miền có thẩm quyền có bảo mật trả về một tham chiếu bao hàm dữ liệu DNSSEC cùng với tập bản ghi tài nguyên NS này.

Khi một tập bản ghi tài nguyên DS có tại điểm chuyển giao, máy chủ tên miền phải trả về cả tập bản ghi tài nguyên DS và (các) bản ghi tài nguyên RRSIG liên kết của nó trong phần thẩm quyền cùng với tập bản ghi tài nguyên NS này.

Khi không có tập bản ghi tài nguyên DS tại điểm chuyển giao, máy chủ tên miền phải trả về cả bản ghi tài nguyên NSEC chỉ ra rằng tập bản ghi tài nguyên DS không có và (các) bản ghi tài nguyên RRSIG liên kết của bản ghi tài nguyên NSEC này cùng với tập bản ghi tài nguyên NS. Máy chủ tên miền phải đặt tập bản ghi tài nguyên NS trước tập bản ghi tài nguyên NSEC và (các) bản ghi tài nguyên RRSIG liên kết của nó.

Việc bao hàm các bản ghi tài nguyên DS, NSEC và RRSIG làm tăng kích cỡ của các bản tin tham chiếu và có thể làm cho một vài hoặc tất cả các bản ghi tài nguyên liên kết bị loại bỏ. Khi không gian không cho phép bao hàm tập bản ghi tài nguyên DS hoặc NSEC và các bản ghi tài nguyên RRSIG liên kết, máy chủ tên miền phải thiết lập bit TC.

***Hồi đáp các truy vấn về các bản ghi tài nguyên DS***

Loại bản ghi tài nguyên DS là khác thường khi nó chỉ xuất hiện về phía zone cha của zone cut. Ví dụ, tập bản ghi tài nguyên DS để chuyển giao “foo.example” được chứa trong zone “example” mà không phải là zone “foo.example”. Điều này yêu cầu các nguyên tắc xử lý đặc biệt đối với cả các máy chủ tên miền và Resolver vì máy chủ tên miền đối với zone con có thẩm quyền đối với tên miền này ở zone cut này theo các nguyên tắc DNS chuẩn nhưng zone con không chứa tập bản ghi tài nguyên DS này.

Security-Aware Resolver gửi các truy vấn đến zone cha khi tìm kiếm một bản ghi tài nguyên DS ở điểm chuyển giao. Tuy nhiên, cần các nguyên tắc đặc biệt để tránh làm nhầm lẫn các Security-Oblivious Resolver , chúng có thể bị liên quan trong việc xử lý một truy vấn như vậy (ví dụ, trong một cấu hình mạng có bắt buộc một Security-Aware Resolver chuyển các truy vấn của nó qua một security-oblivious recursive name server). Phần còn lại của mục này trình bày cách một Security-Aware Name Server xử lý các truy vấn theo trật tự để tránh xảy ra vấn đề này.

Nhu cầu đối với một việc xử lý đặc biệt của một Security-Aware Name Server chỉ phát sinh khi tất cả các điều kiện sau đều thỏa mãn:

* Máy chủ tên miền đã nhận được một truy vấn đối với tập bản ghi tài nguyên DS tại zone cut.
* Máy chủ tên miền có thẩm quyền đối với zone con.
* Máy chủ tên miền không có thẩm quyền đối với zone cha.
* Máy chủ tên miền không thực hiện đệ quy.

Trong tất cả các trường hợp khác, máy chủ tên miền có cách để có tập bản ghi tài nguyên DS này hoặc không cần có tập bản ghi tài nguyên DS này theo các nguyên tắc xử lý không DNSSEC, do đó máy chủ tên miền có thể trả về tập bản ghi tài nguyên DS hoặc một trả lời lỗi theo các nguyên tắc xử lý chuẩn này.

Tuy nhiên, khi tất cả các điều kiện trên được thỏa mãn, máy chủ tên miền có thẩm quyền đối với SNAME nhưng không thể cung cấp tập bản ghi tài nguyên được yêu cầu này. Trong trường hợp này, máy chủ tên miền phải trả về một trả lời có thẩm quyền “không có dữ liệu” chỉ ra rằng tập bản ghi tài nguyên DS không tồn tại trong zone apex của zone con.

* **Hồi đáp các truy vấn đối với loại AXFR hoặc IXFR**

DNSSEC không làm thay đổi quá trình DNS zone transfer. Một Signed Zone sẽ chứa các bản ghi tài nguyên RRSIG, DNSKEY và DS nhưng các bản ghi tài nguyên này không có ý nghĩa đặc biệt đối với một hoạt động của zone transfer.

Không yêu cầu một máy chủ tên miền có thẩm quyền phải kiểm tra xem một zone đã được ký đúng trước khi gửi hoặc nhận một zone transfer.

Tuy nhiên,máy chủ tên miền có thẩm quyền có thể lựa chọn để hủy bỏ một zone transfer khi zone này không thỏa mãn bất kỳ các yêu cầu về ký. Mục đích chính của zone transfer là để đảm bảo rằng tất cả các máy chủ tên miền có các bản sao chép giống nhau của zone. Một máy chủ tên miền có thẩm quyền lựa chọn thực hiện việc xác nhận zone của chính nó không được loại bỏ một số bản ghi tài nguyên và chấp nhận các bản ghi tài nguyên khác một cách có lựa chọn.

Các tập bản ghi tài nguyên DS chỉ xuất hiện ở phía cha của zone cut và là dữ liệu có thẩm quyền trong zone cha. Như với bất kỳ tập bản ghi tài nguyên có thẩm quyền khác, tập bản ghi tài nguyên DS phải được bao hàm trong các zone transfer của zone mà trong zone đó tập bản ghi tài nguyên này là dữ liệu có thẩm quyền. Trong trường hợp tập bản ghi tài nguyên DS, zone đó là zone cha.

Các bản ghi tài nguyên NSEC xuất hiện trong cả zone cha và con ở zone cut và là dữ liệu có thẩm quyền trong cả zone cha và con. Các bản ghi tài nguyên NSEC phía cha và con ở zone cut không giống nhau vì bản ghi tài nguyên NSEC trong zone apex của zone con sẽ luôn luôn chỉ ra sự tồn tại của bản ghi tài nguyên SOA của zone con trong khi bản ghi tài nguyên NSEC phía cha ở zone cut sẽ không bao giờ chỉ ra sự tồn tại của một bản ghi tài nguyên SOA. Như với bất kỳ các bản ghi tài nguyên có thẩm quyền khác, các bản ghi tài nguyên NSEC phải được bao hàm trong các zone transfer của zone mà trong zone đó chúng là dữ liệu có thẩm quyền. bản ghi tài nguyên NSEC phía cha ở zone cut phải được bao hàm trong các zone transfer của zone cha và NSEC ở zone apex của zone con phải được bao hàm trong các zone transfer của zone con.

Các bản ghi tài nguyên RRSIG xuất hiện trong cả zone cha và con ở zone cut và có thẩm quyền trong mỗi zone chứa tập bản ghi tài nguyên có thẩm quyền này mà bản ghi tài nguyên RRSIG cung cấp chữ ký này. Tức là, bản ghi tài nguyên RRSIG dành cho một tập bản ghi tài nguyên DS hoặc một bản ghi tài nguyên NSEC phía cha ở zone cut sẽ có thẩm quyền trong zone cha và bản ghi tài nguyên RRSIG dành cho tập bản ghi tài nguyên bất kỳ trong zone apex của zone con sẽ có thẩm quyền trong zone con. Các bản ghi tài nguyên RRSIG phía cha và con ở zone cut sẽ không bao giờ giống nhau vì trường Name của Signer của một bản ghi tài nguyên RRSIG trong zone apex của zone con sẽ chỉ ra một bản ghi tài nguyên DNSKEY trong zone apex của zone con trong khi trường này của bản ghi tài nguyên RRSIG phía cha ở zone cut sẽ chỉ ra một bản ghi tài nguyên DNSKEY trong zone apex của zone cha. Như với bất kỳ các bản ghi tài nguyên có thẩm quyền khác, các bản ghi tài nguyên RRSIG phải được bao hàm trong các zone transfer của zone mà trong zone đó chúng là dữ liệu có thẩm quyền.

***Các bit AD và CD trong một trả lời có thẩm quyền***

Các bit CD và AD được thiết kế để sử dụng trong truyền tin giữa các Security-Aware Resolver và các Security-Aware Recursive Name Server. Các bit này phần lớn không liên quan đến quá trình truy vấn bởi các máy chủ tên miền có thẩm quyền có bảo mật.

Một Security-Aware Name Server không thực hiện xác thực chữ ký đối với dữ liệu có thẩm quyền trong quá trình truy vấn, thậm chí khi bit CD trống. Security-Aware Name Server nên xóa bit CD này khi tạo một trả lời có thẩm quyền.

Security-Aware Name Server không được thiết lập bit AD trong một trả lời trừ khi máy chủ tên miền này xem tất cả các tập bản ghi tài nguyên trong các phần trả lời và thẩm quyền của trả lời là xác thực. Chính sách địa phương của Security-Aware Name Server có thể xem dữ liệu từ một zone có thẩm quyền là xác thực mà không phải xác thực thêm. Tuy nhiên, máy chủ tên miền này không được làm vậy trừ khi máy chủ tên miền này có được zone có thẩm quyền thông qua các biện pháp bảo mật (ví dụ như cơ chế zone transfer có bảo mật) và không được làm vậy trừ khi hành vì này đã được cấu hình rõ ràng.

Một Security-Aware Name Server mà hỗ trợ đệ quy phải theo các nguyên tắc dành cho các bit CD và AD khi tạo một trả lời có liên qua dữ liệu có được thông qua đệ quy.

### **2.3.2. Máy chủ tên miền đệ quy (Recursive Name Server)**

Security-Aware Recursive Name Server (máy chủ tên miền đệ quy có khả năng nhận thức an toàn) là phần tử hoạt động trong cả vai trò của Security-Aware Name Server và Security-Aware Resolver. Phía Resolver tuân theo các nguyên tắc thông thường để đệm và đệm âm được áp dụng cho bất kỳ Security-Aware Resolver.

* **Bit DO**

Phía Resolver của một Security-Aware Recursive Name Server phải thiết lập bit DO khi gửi các yêu cầu mà không cần để ý tới trạng thái của bit DO trong yêu cầu khởi tạo được phía máy chủ tên miền nhận. Khi bit DO trong truy vấn khởi tạo không được thiết lập, phía máy chủ tên miền phải lấy đi các bản ghi tài nguyên DNSSEC có thẩm quyền bất kỳ từ trả lời nhưng không được lấy đi các loại bản ghi tài nguyên DNSSEC bất kỳ mà truy vấn khởi tạo đã yêu cầu rõ ràng.

* **Bit CD**

Bit CD tồn tại để cho phép Security-Aware Resolver không cho phép việc xác thực chữ ký trong quá trình truy vấn cụ thể của một Security-Aware Name Server.

Phía máy chủ tên miền phải sao chép trạng thái thiết lập của bit CD từ một truy vấn sang trả lời tương ứng.

Phía máy chủ tên miền của Security-Aware Recursive Name Server phải truyền trạng thái của bit CD sang phía Resolver cùng với phần còn lại của một truy vấn khởi tạo sao cho phía Resolver sẽ biết liệu nó có được yêu cầu phải kiểm tra dữ liệu phản hồi mà nó trả về phía máy chủ tên miền. Khi bit CD được thiết lập, nó chỉ ra rằng Resolver gốc sẵn sàng thực hiện bất cứ việc xác thực mà chính sách địa phương của nó yêu cầu. Do đó, phía Resolver của máy chủ tên miền đệ quy này không cần thực hiện xác thực các tập bản ghi tài nguyên trong trả lời. Khi bit CD được thiết lập, máy chủ tên miền đệ quy này nên, nếu có thể, trả về dữ liệu được yêu cầu về Resolver gốc, thậm chí khi chính sách xác thực địa phương của máy chủ tên miền đệ quy này sẽ loại bỏ các bản ghi tài nguyên này trong truy vấn. Do đó, bằng cách thiết lập bit CD, Resolver gốc đã chỉ ra rằng nó có trách nhiệm thực hiện việc xác thực của chính nó và máy chủ tên miền đệ quy không nên can thiệp.

Khi phía Resolver thực hiện BAD cache và phía máy chủ tên miền nhận một truy vấn phù hợp một mục trong BAD cache của phía Resolver, phản ứng của phía máy chủ tên miền phụ thuộc vào trạng thái của bit CD trong truy vấn gốc. Khi bit CD được thiết lập, phía máy chủ tên miền nên trả về dữ liệu từ BAD cache. Khi bit CD không được thiết lập, phía máy chủ tên miền phải trả về RCODE 2 (lỗi máy chủ).

Mục đích của nguyên tắc trên là để cung cấp dữ liệu thô đến các máy khách có khả năng thực hiện các kiểm tra chữ ký của chính chúng đồng thời bảo vệ các máy khách phụ thuộc phía Resolver của Security-Aware Recursive Name Server thực hiện các kiểm tra này. Một số lý do có khả năng mà việc xác thực chữ ký có thể thất bại liên quan các điều kiện có thể không được áp dụng giống nhau đối với máy chủ tên miền đệ quy và máy khách có liên quan. Ví dụ, xung nhịp của máy chủ tên miền đệ quy có thể được thiết lập không chính xác hay máy khách có thể biết một Island of Security có liên quan mà máy chủ tên miền đệ quy không chia sẻ. Trong những trường hợp như vậy, việc “bảo vệ” máy khách có khả năng thực hiện xác thực chữ ký chính nó khỏi việc thấy dữ liệu “xấu” không giúp cho máy khách.

* **Bit AD**

Phía máy chủ tên miền của Security-Aware Recursive Name Server không được thiết lập bit AD trong trả lời trừ khi máy chủ tên miền này xem xét tất cả các tập bản ghi tài nguyên trong các phần trả lời và thẩm quyền là xác thực. Phía máy chủ tên miền nên thiết lập bit AD khi và chỉ khi phía Resolver xem xét tất cả các tập bản ghi tài nguyên trong phần trả lời và bất kỳ các bản ghi tài nguyên phản hồi phủ định có liên quan trong phần thẩm quyền là xác thực. Phía Resolver phải theo đúng thủ tục để xác định liệu các bản ghi tài nguyên này trong truy vấn có xác thực. Tuy nhiên, để tương thích ngược, máy chủ tên miền đệ quy có thể thiết lập bit AD khi trả lời bao hàm các bản ghi tài nguyên CNAME chưa được ký khi các bản ghi tài nguyên CNAME này có thể đã được đồng bộ từ một bản ghi tài nguyên DNAME thẩm quyền mà nó cũng được bao hàm trong trả lời này theo các nguyên tắc đồng bộ. Ví dụ trong các trả lời DNSSEC.

### **2.3.3. Bộ phân giải**

Gồm hoạt động của các thành phần bao hàm các chức năng của Security-Aware Resolver (khả năng nhận biết an toàn). Trong nhiều trường hợp các chức năng này sẽ thuộc Security-Aware Recursive Name Server (máy chủ tên miền đệ quy có khả năng nhận thức an toàn) nhưng một Security-Aware Resolver đơn độc có nhiều yêu cầu giống nhau.

* **Hỗ trợ EDNS**

Security-Aware Resolver phải bao hàm một EDNS OPT giả - bản ghi tài nguyên với bit DO được thiết lập khi gửi các truy vấn.

Security-Aware Resolver phải hỗ trợ kích cỡ bản tin tối thiết 1220 octet nên hỗ trợ kích cỡ bản tin 4000 octet và phải sử dụng trường “sender's UDP payload size” trong EDNS OPT giả-bản ghi tài nguyên để thông báo kích cỡ bản tin mà nó sẵn sàng nhận. lớp ip của Security-Aware Resolver phải xử lý các gói tin UDP được phân đoạn một cách chính xác không cần quan tâm đến các gói tin được phân đoạn này là được nhận thông qua IPv4 hay IPv6.

* **Hỗ trợ kiểm tra chữ ký**

Security-Aware Resolver phải hỗ trợ các cơ chế kiểm tra chữ và nên áp dụng chúng cho mỗi trả lời nhận được trừ khi:

* Security-Aware Resolver thuộc Security-Aware Recursive Name Server và trả lời là kết quả của đệ quy dựa vào một truy vấn nhận được với bit CD được thiết lập.
* Trả lời là kết quả của một đệ quy được tạo trực tiếp thông qua một dạng giao diện ứng dụng hướng dẫn Security-Aware Resolver không được thực hiện xác thực đối với truy vấn này.
* Việc xác thực đối với truy vấn này được chính sách nội bộ ngăn chặn.
* Việc hỗ trợ kiểm tra chữ ký của một Security-Aware Resolver phải bao hàm việc hỗ trợ kiểm tra các tên miền chủ ký tự đại diện.

Các Security-Aware Resolver có thể truy vấn các bản ghi tài nguyên bảo mật thiếu trong một nỗ lực để thực hiện xác thực. Các hành động để thực hiện điều này phải biết rằng các trả lời nhận được có thể không đủ để xác thực trả lời gốc. Ví dụ, việc cập nhật zone có thể đã làm thay đổi (xóa) thông tin cần thiết giữa các truy vấn gốc và kế tiếp.

Khi cố gắng lấy lại các bản ghi tài nguyên NSEC thiếu đặt ở phía cha ở zone cut, một Security-Aware Resolver chế độ lặp phải truy vấn các máy chủ tên miền về zone cha mà không phải là zone con.

Khi cố gằng lấy lại một DS thiếu, Security-Aware Resolver chế độ lặp phải truy vấn các máy chủ tên miền về zone cha mà không phải là zone con. Các Security-Aware Name Server cần áp dụng các nguyên tắc xử lý đặc biệt để xử lý bản ghi tài nguyên DS này và trong một số tình huống, Resolver cũng có thể cần áp dụng các nguyên tắc đặc biệt để định vị các máy chủ tên miền này cho zone cha khi Resolver này không có tập bản ghi tài nguyên NS phía cha. Để định vị tập bản ghi tài nguyên NS phía cha, Resolver có thể bắt đầu với tên miền chuyển giao, loại bỏ nhãn ngoài cùng bên trái và truy vấn một tập bản ghi tài nguyên NS bằng tên miền đó. Khi không có tập bản ghi tài nguyên NS có ở tên miền đó, tiếp theo Resolver loại bỏ nhãn còn lại ngoài cùng bên trái và thử truy vấn đối với tên miền đó, lặp lại quá trình đi này cho tới khi tìm thấy tập bản ghi tài nguyên NS hoặc không còn nhãn nào.

* **Xác định trạng thái bảo mật của dữ liệu**

Security-Aware Resolver phải có khả năng xác định liệu nó có nên chờ đợi một tập bản ghi tài nguyên cụ thể được ký. Một cách chính xác hơn, Security-Aware Resolver phải có khả năng phân biệt giữa 4 trường hợp sau:

* *Bảo mật*: Tập bản ghi tài nguyên mà Resolver có khả năng xây dựng một chuỗicác bản ghi tài nguyên DNSKEY và DS được ký từ một anchor bảo mật tin cậy đến tập bản ghi tài nguyên này. Trong trường hợp này, tập bản ghi tài nguyên này nên được ký và phụ thuộc vào xác nhận chữ ký.
* *Không bảo mật*: Tập bản ghi tài nguyên mà Resolver biết rằng nó không cóchuỗi các bản ghi tài nguyên DNSKEY và DS được ký từ bất kỳ điểm khởi điểm tin cậy đến tập bản ghi tài nguyên này. Điều này có thể xảy ra khi tập bản ghi tài nguyên đích nằm trong một zone không được ký hoặc một zone không được ký con cháu. Trong trường hợp này, tập bản ghi tài nguyên này có thể hoặc không được ký nhưng Resolver sẽ không thể kiểm tra chữ ký.
* *Giả mạo*: Tập bản ghi tài nguyên mà Resolver tin cậy rằng nó có thể thiết lậpmột chuỗi tin cậy nhưng nó lại không thể thực hiện điều đó vì chữ ký không được xác nhận vì một lý do nào đó hoặc vì dữ liệu thiếu mà các bản ghi tài nguyên DNSSEC có liên quan chỉ ra nên có. Trường hợp này có thể chỉ ra một tấn công nhưng cũng có thể chỉ ra một lỗi cấu hình hoặc một dạng lỗi dữ liệu.
* *Không xác định*: Tập bản ghi tài nguyên mà Resolver không thể xác định liệutập bản ghi tài nguyên này có nên được ký vì Resolver không thể có các bản ghi tài nguyên DNSSEC cần thiết. Điều này có thể xảy ra khi Security-Aware Resolver không thể liên lạc với các Security-Aware Name Server đối với các zone liên quan.

**Trust Anchor được cấu hình**

Security-Aware Resolver phải có khả năng được cấu hình với ít nhất khóa công khai tin cậy hoặc bản ghi tài nguyên DS nên có khả năng được cấu hình với nhiều khóa công khai tin cậy hoặc các bản ghi tài nguyên DS. Vì Security-Aware Resolver sẽ không có khả năng xác nhận các chữ ký không có một Trust Anchor được cấu hình như vậy, Resolver nên có một cơ chế chắc chắn hợp lý nào đó để đạt được các khóa này khi nó khởi tạo; ví dụ một cơ chế như vậy sẽ là một dạng lưu trữ không khả biến (như một ổ đĩa) hoặc một dạng của cơ chế cấu hình mạng nội bộ tin cậy nào đó.

Chú ý rằng các Trust Anchor cũng che đậy thông tin khóa được cập nhật theo một cách bảo mật. Cách thức bảo mật này có thể thông qua phương tiện vật lý, giao thức trao đổi khóa hoặc một số biện pháp khác.

* **Phản hồi của bộ đệm**

Một Security-Aware Resolver nên lưu bộ nhớ đệm cho mỗi phản hồi như một mục đơn nguyên chứa toàn bộ câu trả lời, bao gồm cả tên miền tập bản ghi tài nguyên và bất kỳ bản ghi tài nguyên DNSSEC được liên kết. Resolver nên loại bỏ toàn bộ mục đơn nguyên này khi có bất kỳ bản ghi tài nguyên chứa trong nó bị hết hạn. Trong phần lớn trường hợp, chỉ mục nhớ đệm phù hợp đối với mục nhập nguyên này sẽ là bội ba <QNAME, QTYPE, QCLASS> nhưng trong các trường hợp như dạng đệ quy chỉ mục nhớ đệm phù hợp sẽ là bội hai <QNAME, QCLASS>.

Lý do đối với các khuyến nghị này là giữa truy vấn ban đầu và hết thời gian dữ liệu trong nhớ đệm, dữ liệu có thẩm quyền có thể đã thay đổi (ví dụ, thông qua cập nhật động)

Có 2 tình huống liên quan:

* Bằng cách sử dụng bản ghi tài nguyên RRSIG, có thể suy diễn rằng một trả lời đã được đồng bộ từ một ký tự đại diện. Security-Aware Recursive Name Server có thể lưu trữ dữ liệu ký tự đại diện này và sử dụng nó để tạo các phản hồi khẳng định đối với các truy vấn chứ không phải là tên miền mà trả lời gốc đã được nhận đầu tiên.
* Các bản ghi tài nguyên NSEC nhận được để chỉ ra sự không tồn tại của một tên miền có thể được Security-Aware Resolver sử dụng lại để chỉ ra sự không tồn tại của bất kỳ tên miền trong dải tên miền nó bao trùm.

Trong lý thuyết, một Resolver có thể sử dụng các ký tự đại diện hoặc các bản ghi tài nguyên NSEC để tạo các phản hồi khẳng định và phủ định (tương ứng) cho tới khi TTL hoặc các chữ ký trên các bản ghi tài nguyên trong truy vấn hết thời gian. Tuy nhiên, các Resolver nên thận trọng để tránh việc ngăn chặn dữ liệu có thẩm quyền mới hoặc việc đồng bộ dữ liệu mới trên chính nó. Các Resolver theo khuyến nghị này sẽ có quan điểm nhất quán hơn về không gian tên miền.

* **Xử lý các bit CD và AD**

Security-Aware Resolver có thể thiết lập bit CD của truy vấn để chỉ ra rằng Resolver này nhận trách nhiệm thực hiện bất kỳ thẩm quyền mà chính sách nội bộ của nó yêu cầu đối với các tập bản ghi tài nguyên trong trả lời này. Security-Aware Resolver phải xóa bit AD khi xây dựng các bản tin truy vấn để bảo vệ chống lại các máy chủ tên miền có nhiều lỗi sao chép các bit phần mào đầu một cách máy móc mà chúng không hiểu từ bản tin truy vấn sang bản tin trả lời.

Resolver phải không quan tâm đến ý nghĩa của các bit CD và AD trong một trả lời trừ khi trả lời này đã đạt được bằng cách sử dụng một kênh có bảo mật hoặc Resolver này đã được cấu hình một cách đặc biệt để quan tâm các bit phần mào đầu bản tin mà không sử dụng kênh có bảo mật.

* **Dữ liệu bộ đệm BAD**

Khi nhiều lỗi xác thực là tạm thời, một số lỗi có thể liên tục, như thể chúng là do lỗi quản lý gây ra (lỗi ký lại một zone, lệch xung nhịp, …). Vì việc truy vấn lại sẽ không có ích trong các trường hợp này, các Resolver xác thực có thể tạo một lượng lưu lượng DNS không cần thiết đáng kể khi lặp lại các truy vấn đối với các tập bản ghi tài nguyên với các lỗi xác thực liên tục này.

Để tránh lưu lượng DNS không cần thiết này, các Security-Aware Resolver có thể nhớ đệm dữ liệu với các chữ ký không hợp pháp bằng một số hạn chế.

Về mặt khái niệm, việc nhớ đệm dữ liệu này tương tự việc nhớ đệm âm ngoại trừ rằng thay vi nhớ đệm một phản hồi phủ định hợp pháp, Resolver này đang nhớ đệm sự kiện một trả lời cụ thể xác thực không thành công. Tiêu chuẩn này xem việc nhớ đệm dữ liệu có các chữ ký không hợp pháp là một “BAD cache”.

Các Resolver thực hiện một BAD cache phải thực hiện các bước để tránh nhớ đệm khỏi trở thành một thiết bị tăng cường hữu hiệu của tấn công từ chối dịch vụ, cụ thể là:

Khi các tập bản ghi tài nguyên xác thực không thành công không có các TTL tin cậy, việc thực hiện này phải ấn định một TTL. TTL này nên nhỏ để giảm thiểu ảnh hưởng của nhớ đệm các kết quả của một tấn công.

Để tránh nhớ đệm một lỗi xác thực tạm thời (nó có thể là kết quả của một tấn công), các Resolver nên theo dấu các truy vấn gây ra các lỗi xác thực và chỉ nên trả lời từ BAD cache sau khi số lượt trả lời các truy vấn đối với <QNAME, QTYPE, QCLASS> cụ thể xác thực không thành công vượt quá một giá trị ngưỡng.

Các Resolver không được trả về các tập bản ghi tài nguyên từ BAD cache trừ khi Resolver này không được yêu cầu để xác nhận các chữ ký của các tập bản ghi tài nguyên trong câu hỏi

* **Các CNAME được đồng bộ**

Một Security-Aware Resolver xác nhận phải xử lý chữ ký của một bản ghi tài nguyên DNAME được ký hợp pháp cũng như bao trùm các bản ghi tài nguyên CNAME chưa được ký có thể đã được đồng bộ từ bản ghi tài nguyên, ít nhất ở mức không hủy bỏ chỉ có một bản tin trả lời vì nó chứa các bản ghi tài nguyên CNAME như vậy. Resolver này có thể giữ lại các bản ghi tài nguyên CNAME này trong nhớ đệm của nó hoặc trong các trả lời mà nó truyền trở lại nhưng nó không được yêu cầu làm vậy.

* **Các Stub Resolver**

Security-Aware Stub Resolver phải hỗ trợ các loại bản ghi tài nguyên DNSSEC ít nhất ở mức không xử lý nhầm các trả lời chỉ vì chúng chứa các bản ghi tài nguyên DNSSEC.

* **Xử lý bit DO**

Non-validating security-aware stub resolver có thể chứa các bản ghi tài nguyên DNSSEC được Security-Aware Recursive Name Server trả về như là dữ liệu mà Stub Resolver này truyền lại cho ứng dụng liên quan đến nó nhưng có không được yêu cầu làm vậy. Non-validating stub resolver tìm cách làm này sẽ cần thiết lập bit DO để nhận các bản ghi tài nguyên DNSSEC từ máy chủ tên miền đệ quy này.

Validating Security-Aware Stub Resolver phải thiết lập bit DO vì nếu không nó sẽ không nhận các bản ghi tài nguyên DNSSEC mà nó cần thực hiện xác nhận chữ ký.

* **Xử lý bit CD**

Non-validating security-aware stub resolver không nên thiết lập bit CD khi gửi các truy vấn trừ khi nó được lớp ứng dụng yêu cầu, như theo định nghĩa, Non-Validating Stub Resolver phụ thuộc vào Security-Aware Recursive Name Server thực hiện xác thực thay cho nó.

Validating Security-Aware Stub Resolver nên thiết lập bit CD vì nếu không Security-Aware Recursive Name Server sẽ trả lời truy vấn bằng cách sử dụng chính sách nội bộ của máy chủ tên miền này, chính sách này có thể ngăn cản Stub Resolver này nhận dữ liệu có thể được chấp nhận theo chính sách nội bộ của Stub Resolver này.

* **Xử lý bit AD**

Non-validating security-aware stub resolver có thể lựa chọn để kiểm tra việc thiết lập của bit AD trong các bản tin phản hồi mà nó nhận để xác định liệu Security-Aware Recursive Name Server gửi các xác nhận phản hồi đã được kiểm tra mã hóa dữ liệu trong các phần trả lời và thẩm quyền của bản tin phản hồi. Tuy nhiên, chú ý rằng, các phản hồi được Security-Aware Stub Resolver nhận phụ thuộc chủ yếu vào chính sách nội bộ của Security-Aware Recursive Name Server. Do đó, có thể có ít giá trị thực tế trong việc kiểm tra trạng thái của bit AD ngoại trừ có thể trợ giúp gỡ rối. Trong bất kỳ trường hợp nào, Security-Aware Stub Resolver không được đặt bất kỳ tin cậy nào vào xác nhận chữ ký được thực hiện thay thế cho nó trừ khi Security-Aware Stub Resolver này có được dữ liệu này từ Security-Aware Recursive Name Server thông qua một kênh bảo mật.

Validating Security-Aware Stub Resolver không nên kiểm tra việc thiết lập bit AD trong các bản tin phản hồi như theo định nghĩa, Stub Resolver thực hiện xác nhận chữ ký của chính nó mà không quan tâm đến việc thiết lập của bit AD.

### **2.3.4. Hỗ trợ xác thực DNS**

Để sử dụng các bản ghi tài nguyên DNSSEC để xác thực, Security-Aware Resolver yêu cầu biết được cấu hình của ít nhất một bản ghi tài nguyên DNSKEY hoặc DS được xác thực. Quá trình có được và xác thực Trust Anchor khởi đầu này đạt được thông qua một cơ chế bên ngoài nào đó. Ví dụ, Resolver có thể sử dụng việc trao đổi được xác thực ngoại tuyến nào đó để có được một DNSKEY của zone hoặc có được một bản ghi tài nguyên DS nhận biết và xác thực một bản ghi tài nguyên DNSKEY của zone.

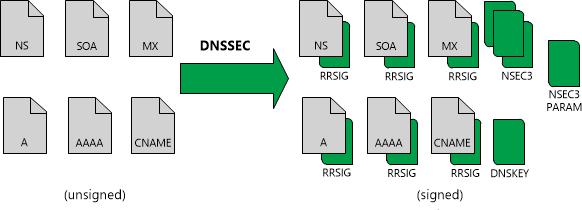
Một bản ghi tài nguyên DNSKEY khởi đầu có thể được sử dụng để xác thực tập bản ghi tài nguyên DNSKEY của zone apex của zone. Để xác thực tập bản ghi tài nguyên DNSKEY của zone apex bằng cách sử dụng một khóa khởi đầu, Resolver này phải:

Kiểm tra xem bản ghi tài nguyên DNSKEY khởi tạo xuất hiện trong tập bản ghi tài nguyên DNSKEY của zone apex và xem bản ghi tài nguyên DNSKEY có Zone KEY Flag (DNSKEY RDATA bit 7) được thiết lập.

Kiểm tra xem có bản ghi tài nguyên RRSIG nào bao trùm tập bản ghi tài nguyên DNSKEY của zone apex và xem kết hợp của bản ghi tài nguyên RRSIG và bản ghi tài nguyên DNSKEY khởi tạo này xác thực tập bản ghi tài nguyên DNSKEY này.

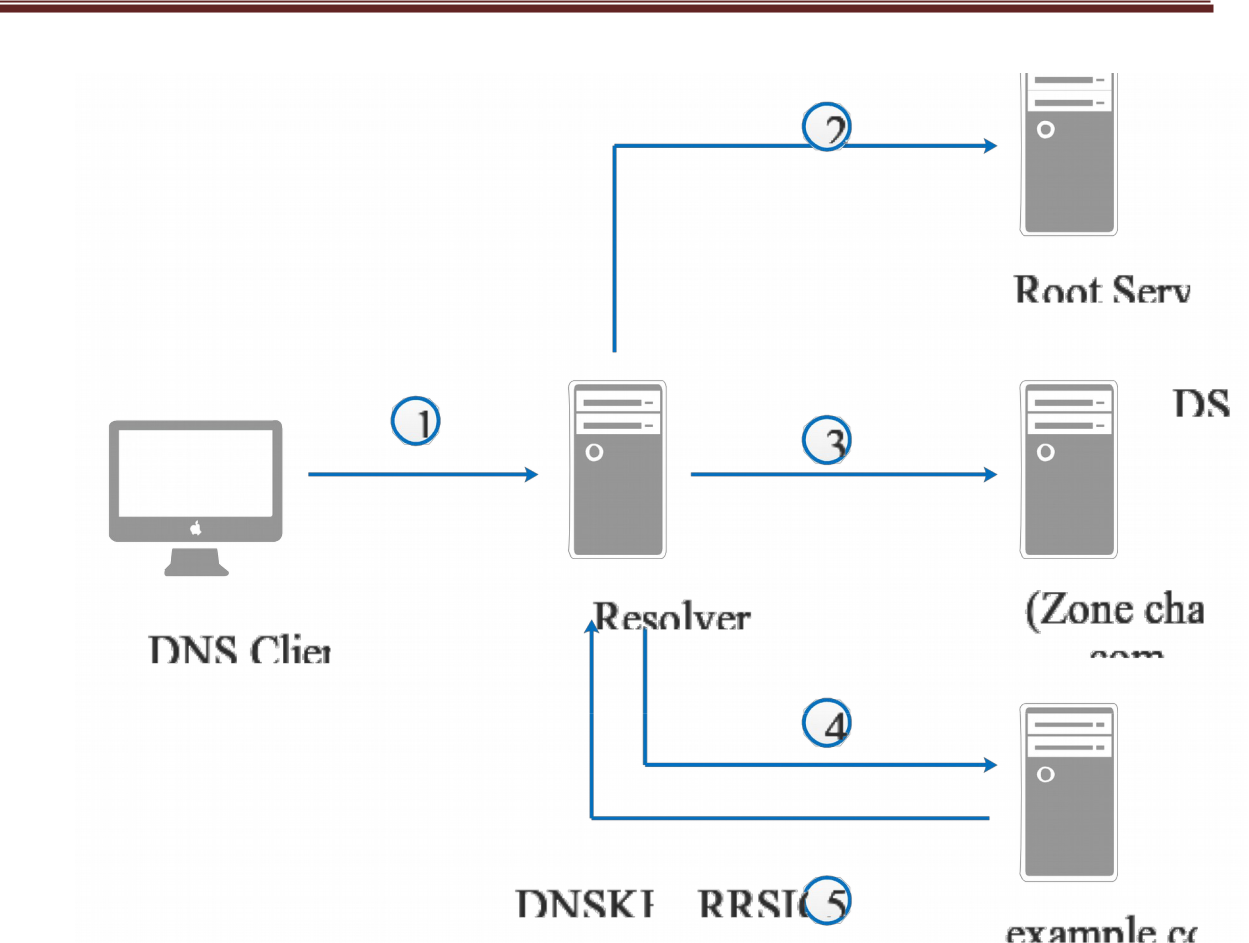
#### ***2.3.4.1.*** ***Quá trình xác nhận tính hợp lệ trong DNSSEC***

Trong DNSSEC, việc xác nhận tính hợp lệ của các hồi đáp DNS được thực hiện thông qua các chữ ký số. Các chữ ký số này được chứa trong các bản ghi tài nguyên DNSSEC, được tạo ra và bổ sung vào zone khi ký zone.

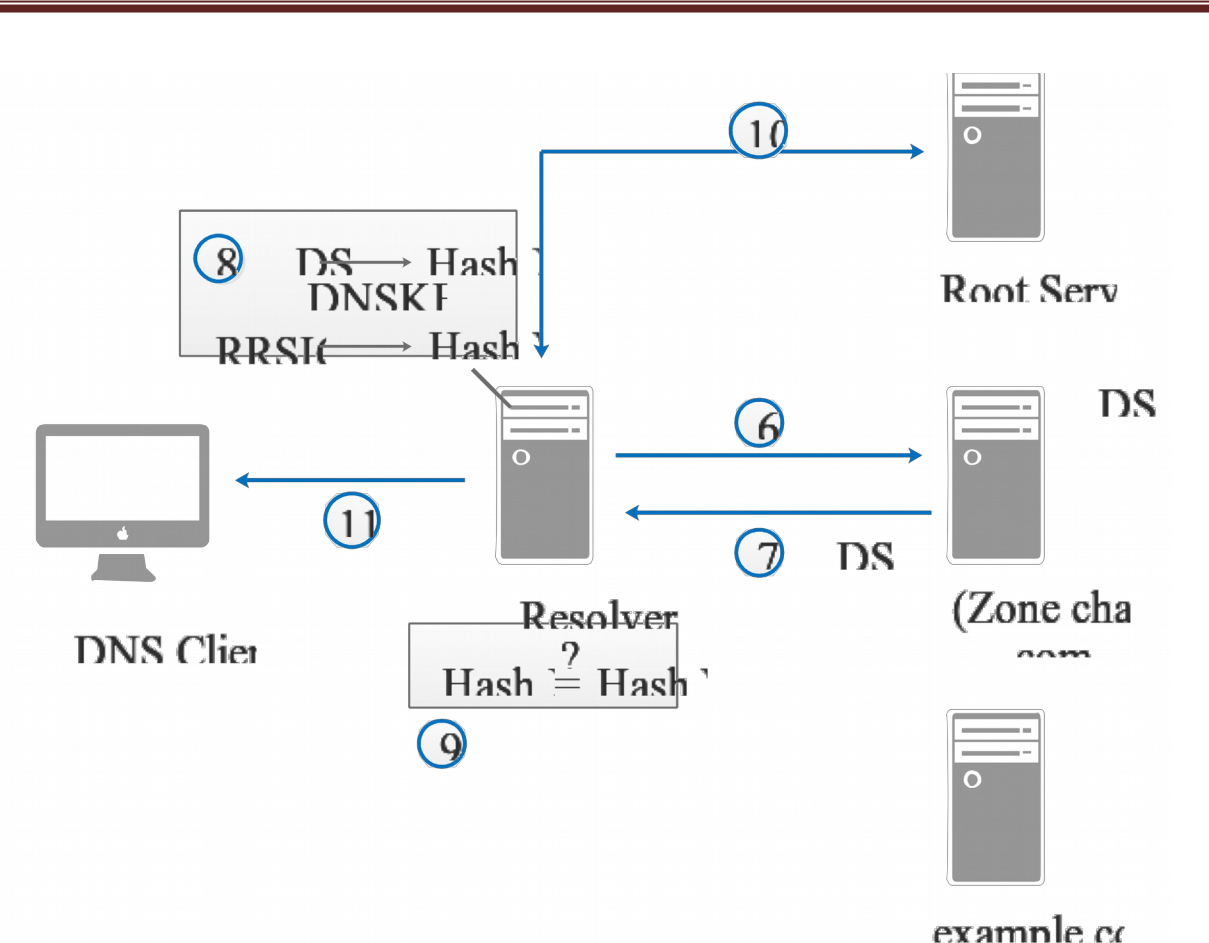


Một quá trình xác nhận tính hợp lệ các hồi đáp DNS sử dụng chữ ký số như sau:

1. Khi Client gửi truy vấn tìm kiếm địa chỉ [www.example.com](http://www.example.com/) tới Resolver.
2. Resolver sẽ truy vấn đến các Root Máy chủ để hỏi tên miền example.com và Root Máy chủ sẽ hướng dẫn Resolvertruy vấn đến máy chủ tên miền quản lý trực tiếp của tên miền example.com cần tìm.
3. Sau đó, Resolver truy vấn đến máy chủ tên miền .com (zone cha) để hỏi example.com, máy chủ tên miền .com sẽ hướng dẫn Resolvertruy vấn đến thẳng Máy chủ tên miền chịu trách nhiệm tên miền example.com
4. Resolver tiếp tục truy vấn đến máy chủ tên miền example.com để hỏi địa chỉ www.example.com.



1. Lúc này,máy chủ tên miền example.com sẽ kiểm tra trong zone và thấy có bản ghi www, máy chủ tên miền example.com sẽ trả lời lại Resolver bằng gói tin hồi đáp DNS bao gồm địa chỉ IP kèm theo DNSKEY và chữ ký số RRSIG.
2. Sau khi Resolver nhận được gói tin hồi đáp DNS, lúc này nó cần phải kiểm tra xem dữ liệu hồi đáp DNS có phải đúng domáy chủ tên miền example.com gửi hay không bằng cách truy vấn lên zone cha (tức máy chủ tên miền .com).
3. Máy chủ tên miền .com sẽ tìm kiếm trong zone file .com và gửi DS (bản ghi chữ ký chuyển giao) về cho Resolver.
4. Sau khi nhận được DS, Resolver thực hiện kiểm tra tính xác thực và toàn vẹn thông qua bộ kiểm tra tính hợp lệ, lấy khóa công khai (từ DNSKEY trong gói tin hồi đáp DNS) đem đi Hash với DS. Và ra một giá trị Hash X.Tiếp tục, Resolver lấy khóa công khai từ DNSKEY giải mã chữ ký số RRSIG được một giá trị Hash Y.



1. Đem so sánh giá trị Hash X với Hash Y xem có bằng nhau không, nếu bằng nhau thì dữ liệu là chính xác. Nếu không bằng nhau, Resolver sẽ gửi về bản tin

SERVFAIL.

1. Sau khi xác định giá trị Hash bằng nhau, Resolver sẽ xét các thông tin trong RRSIG (bao gồm thời gian RRSIG, Time To Live) lại một lần nữa với máy chủ Root.
2. Sau khi đã xác minh, lúc này dữ liệu đã hoàn toàn chính xác, máy chủ Root cho phép Resolver gửi dữ liệu về cho Client truy vấn.

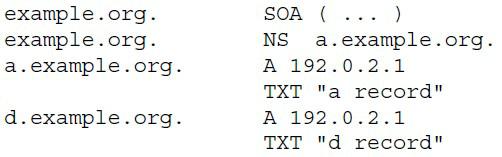
#### ***2.3.4.2.*** ***Cơ chế xác thực từ chối sự tồn tại trong DNSSEC***

Cơ chế xác thực từ chối sự tồn tại cho phép một Resolver xác nhận hợp lệ một tên miền cụ thể nào đó không tồn tại. Cơ chế cũng sử dụng thông báo rằng một tên miền tồn tại nhưng không có kiểu bản ghi tài nguyên cụ thể mà đối tượng đang tìm kiếm. Khi một hồi đáp DNSSEC phủ định (gồm hồi đáp NXDOMAIN và NODATA) được khai báo, một máy chủ tên thường bao gồm 2 bản ghi NSEC. Đối với trường hợp sử dụng NSEC3 (sử dụng hàm băm) sẽ có 3 bản ghi được sử dụng trong hồi đáp đó. Và từ chối sự tồn tại được xác thực sẽ sử dụng phương thức mã hóa để ký các hồi đáp phủ định đó.

* **Từ chối sự tồn tại**

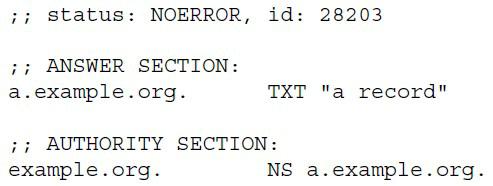
Để có thể hiểu một cách cơ bản về cơ chế từ chối sự tồn tại, một ví dụ sẽ được đưa ra trong DNS như sau:

* Một zone DNS nhỏ với 3 tên miền lần lượt “example.org”, “a.example.org” và “d.example.org”.
* Bốn Type bản ghi gồm: SOA, NS, A và TXT, trong đó bản ghi SOA được viết thu gọn lại.

****

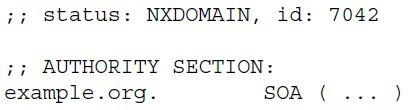
Đây là một zone không ký. Nếu một Resolver gửi truy vấn máy chủ quản lý zone này về tên miền “a.example.org” với Type TXT, thì nó sẽ gửi truy vấn có dạng như sau: “a.example.org TXT”.

Khi đó, máy chủ sẽ tìm kiếm trong dữ liệu zone của nó và tạo ra hồi đáp trả lời. Trong trường hợp này, đây là một câu trả lời khẳng định rằng: “Có, tên miền có tồn tại và đây là dữ liệu”.



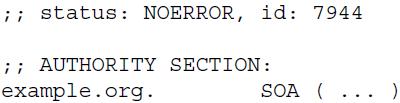
Thông báo “status: NOERROR” cho thấy không phát sinh lỗi khi tìm dữ liệu và trả lời, “id” có giá trị nguyên cho thấy hồi đáp phù hợp với truy vấn. Trong phần ANSWER, có nội dung thông tin cho truy vấn. Phần AUTHORITY giữ các tên của máy chủ tên miền có thông tin liên quan tới zone “example.org”.

Trong trường hợp, Resolver truy vấn về “b.example.org TXT”, nó sẽ nhận được hồi đáp là tên miền cần tìm không tồn tại:



Và trong trường hợp này, trong hồi đáp không có phần ANSWER, trạng thái được thiết lập là NXDOMAIN. Từ đó, Resolver kết luận là “b.example.org” không tồn tại. Phần AUTHORITY giữ bản ghi SOA của “example.org” để Resolver có thể sử dụng nhằm lưu vào hồi đáp phủ định. Khi đó, ta có từ chối sự tồn tại.

Một trường hợp nữa, đó là tên miền có thể tồn tại nhưng Type bản ghi tìm kiếm có thể không tồn tại. Trường hợp biểu diễn sự không tồn tại đó được gọi là hồi đáp NODATA. Khi một Resolver hỏi máy chủ tên miền về “a.example.org AAAA”, sẽ nhận được hồi đáp:



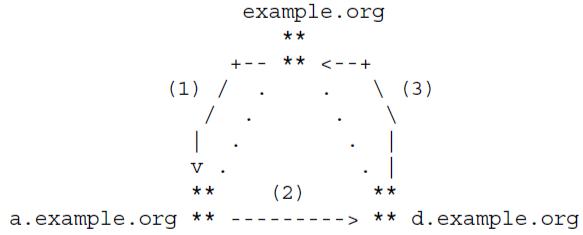
Trạng thái status: NOERROR cho biết tên miền “a.axample.org” tồn tại nhưng trong hồi đáp không chứa phần ANSWER. Đây là một hồi đáp NODATA, có chút khác biệt so với hồi đáp NXDOMAIN. Khi đó, Resolver sẽ kết luận rằng tên miền “a.example.org” tồn tại nhưng không có Type bản ghi “AAAA”.

* **Xác thực từ chối sự tồn tại**

Có thể thấy, trong DNS, máy chủ tên miền có thể tự do trả lời và thực hiện ký, tất nhiên vẫn đảm bảo yêu cầu “ký trước, gửi sau”. Tuy nhiên, khi phát triển theo DNSSEC, cần thiết phải có thêm phần xác thực từ chối sự tồn tại nhằm chứng thực và toàn vẹn cho dữ liệu trao đổi. Một bản ghi bảo mật kế tiếp NSEC được giới thiệu trong DNSSEC.

So với DNS, tên các Type trong DNSSEC được đổi sang tên mới: SIG được đổi thành RRSSIG, KEY được đổi thành DNSKEY. Bản ghi NSEC được sử dụng để thông tin cho Resolver biết các bản ghi có tên miền nằm trong khoảng trống giữa các tên miền hiện diện là không tồn tại trong zone, đồng thời cho biết Type của bản ghi tài nguyên hiện diện trong một tên miền hiện thời.

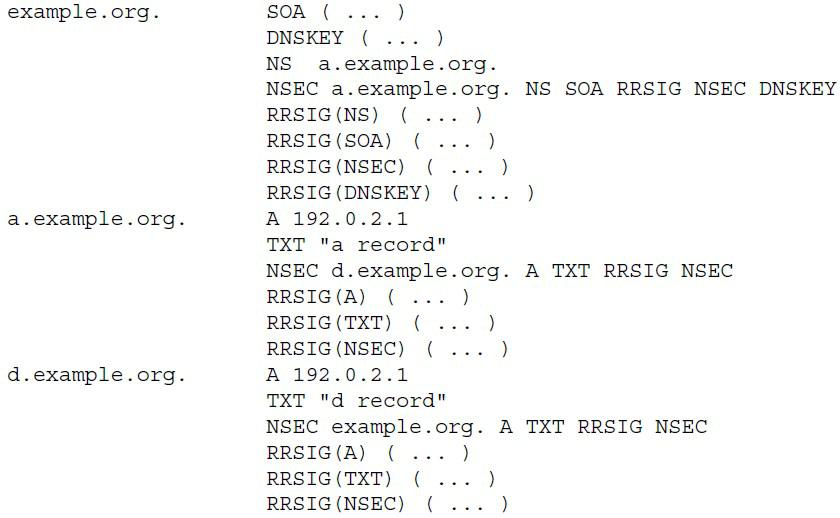
Để hiểu rõ hơn về cách thức làm việc của NSEC, một zone “example.org” được tạo ra và sắp xếp theo thứ tự chính tắc như sau:



Ba bản ghi NSEC được bổ sung cho mỗi tên miền và mỗi NSEC sẽ bao hàm khoảng nằm giữa 2 tên miền:

* NSEC thứ nhất (1) bao hàm khoảng nằm giữa tên miền “example.org” và “a.example.org”.
* NSEC thứ hai (2) bao hàm khoảng nằm giữa tên miền “a.example.org” và “d.example.org”.
* NSEC thứ ba (3) bao hàm khoảng nằm giữa tên miền “d.example.org” và “example.org”.

Zone được tạo ra trong ví dụ là một zone đã ký trong máy chủ tên miền, có phần nội dung như sau:



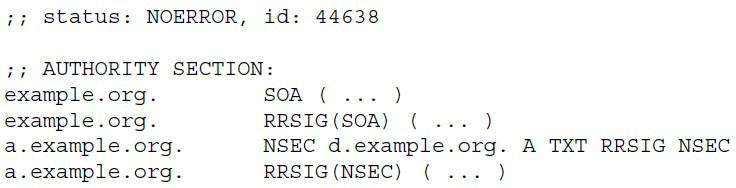
Trong zone này, các bản ghi ký tài nguyên RRSIG và bản ghi NSEC được bổ sung. Nội dung các bản ghi SOA, DNSKEY và RRSIG được viết ngắn gọn lại.

Nếu một Resolver nhận thực được DNSSEC truy vấn tên miền “b.example.org”, nó sẽ nhận lại bản tin với trạng thái “status: NXDOMAIN”, tức là tên miền không tồn tại. Đồng thời, để đảm bảo việc Resolver nhận biết tên miền không tồn tại một cách an toàn thì phải có một bản ghi NSEC đã ký bao hàm không gian tên miền “b.example.org”. Sau đó, khi chữ ký bản ghi NSEC được xác thực hợp lệ, thì tên miền “b.example.org” mới được chứng thực là không tồn tại. Khi đó, ta có xác thực từ chối sự tồn tại.

Trường hợp bị tấn công giả mạo DNS, kẻ tấn công có thể gửi lại hồi đáp NXDOMAIN khi ta truy vấn tìm kiếm tên miền “c.example.org”. Tuy nhiên, điều đó không đem đến bất kỳ tổn hại nào do đã được chứng thực rằng hồi đáp đúng phù hợp với truy vấn.

Các bản ghi NSEC cũng được sử dụng trong các hồi đáp NODATA. Trong trường hợp này, nó liên quan đến Type bitmap khi mà Type bitmap trong bản ghi NSEC cho biết Type của tên miền. Nếu nhìn vào bản ghi NSEC của tên miền“a.example.org”, có thấy các Type gồm: A, TXT, NSEC và RRSIG. Vậy, điều đó cho thấy rằng đối với tên miền “a”, phải có một bản ghi A, TXT, NSEC và RRSIG trong zone.

Một Resolver có thể biết tên miền tồn tại nhưng Type chưa chắc đã tồn tại. Ví dụ, khi một Resolver truy vấn “a.example.org AAAA”, nó sẽ nhận được hồi đáp:



Kiểm tra phần AUTHORITY có thể kết luận:

* Tên miền “a.example.org” tồn tại (do bản ghi NSEC đi kèm với tên miền).
* Type AAAA không tồn tại do không có trong danh sách Type bitmap của NSEC.

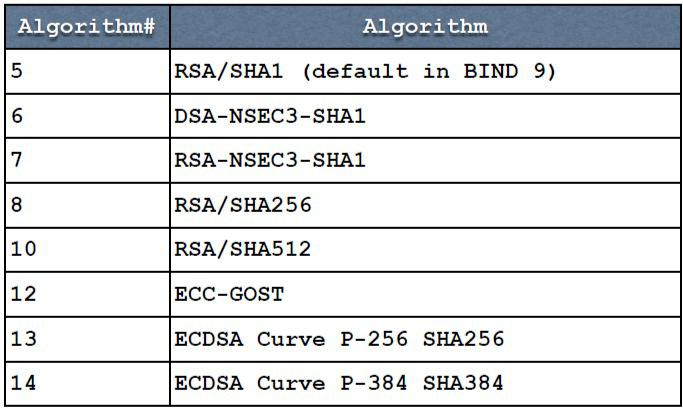
Việc sử dụng hàm băm giải quyết được vấn đề zone walking của NSEC. Tuy nhiên vấn còn một vấn đề nữa cần giải quyết, đó là chi phí cao khi bảo mật một chuyển giao của một zone không an toàn. Cách giải quyết là sử dụng Opt-Out.

Khi sử dụng Opt-Out, các tên miền là một chuyển giao không an toàn và không yêu cầu một bản ghi NSEC3. Thay vào đó, đối với mỗi chuyển giao không an toàn, kích thước zone có thể được giảm với ít nhất hai bản ghi: một bản ghi NSEC3 và một bản ghi RRSIG tương ứng (so với zone ký đầy đủ mà không sử dụng Opt-Out).

* **Thuật toán hàm băm**

NSEC3 sử dụng mã hóa hàm băm cho tất cả các tên miền, bao gồm cả tên miền gốc. Thuật toán được sử dụng cho mã hóa hàm băm là thuật toán SHA1, làm tăng tính bảo mật và độ khó cho các đối tượng tấn công.

Trong tiêu chuẩn này là tiêu chuẩn bổ sung 2 định danh mới (chứ không phải 2 thuật toán mới) cho 2 thuật toán đang sử dụng: Thuật toán 6, DS-NSEC3-SHA1 tương ứng thuật toán 3, DSA. Thuật toán 7, RSASHA1-NSEC3-SHA1 tương ứng thuật toán 5, RSASHA1. Và các định danh thuật toán mới được sử dụng cùng với thuật toán hàm băm NSEC3 SHA1.



Việc tính toán mã hóa băm sử dụng ba trường NSEC3 RDATA là: Hash Algorithm, Salt và Iterations.

Gọi H(x) là hàm băm của x bằng cách sử dụng trường Hash Algorithm được bản ghi tài nguyên NSEC3 lựa chọn, k là số lần lặp và || biểu thị sự kết nối. Khi đó:

*IH(salt, x, 0) = H(x || salt),*

*IH(salt, x, k) = H(IH(salt, x, k-1) || salt), nếu k > 0*

Mã băm của một tên miền được tính toán như sau:

*IH(salt, tên miền, iteration)*

Trong đó tên miền dạng chính tắc được định nghĩa như sau:

Định dạng của tên miền:

Tên miền được mở rộng hoàn toàn (không phụ thuộc tên DNS) và đúng qui định.

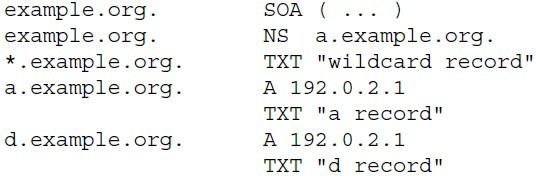
Tất cả chữ Hoa US-ASCII được thay bằng chữ thường US-ASCII.

Nếu tên miền là một tên dưới dạng ký tự đại diện, thì trong định dạng không mở rộng gốc, tên miền bao gồm nhãn “ **\*** ” (không thay thế ký tự đại diện).

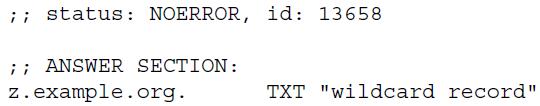
* **Ký tự đại diện**

Một bản ghi ký tự đại diện là một bản ghi nằm trong một zone, được sử dụng khi có các yêu cầu phối hợp với các tên miền không tồn tại. Bản ghi ký tự đại diện sử dụng dấu “\*” phía ngoài cùng bên trái của một tên miền.

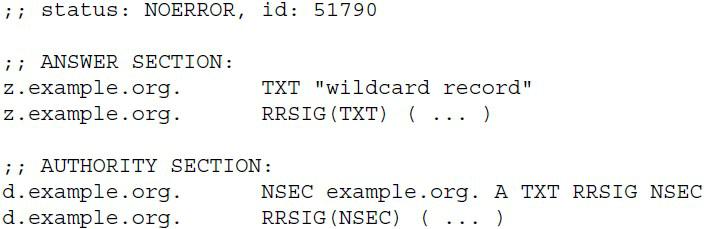
Ví dụ, \*.example.org. là một bản ghi ký tự đại diện.

Từ chối sự tồn tại thường trong các hồi đáp phủ định. Tuy nhiên, từ chối sự tồn tại cũng xuất hiện trong hồi đáp khẳng định, trong đó, phần ANSWER của hồi đáp là không rỗng. Điều này thực hiện được là nhờ có ký tự đại diện.

Ta có một zone chứa một bản ghi ký tự đại diện như trên. Khi một Resolver truy vấn tên miền “z.example.org TXT”, máy chủ tên miền sẽ trả lời với một ký tự đại diện mở rộng thay cho NXDOMAIN:



Khi xét trường hợp trên trong DNSSEC, hồi đáp từ máy chủ tên miền sẽ như sau:



RRSIG trong bản ghi “z.example.org” chỉ cho biết một ký tự đại diện được cấu hình. Thực chất, ký của tên miền “z.example.org” là không tồn tại cũng như không được tạo ra. Thay vào đó, nó chỉ cho biết cho tên miền ký tự đại diện “\*.example.org” được cấu hình và nó đại diện cho tên miền “z.example.org”.

## 2.4. Kết luận

Chương 2 là các nghiên cứu về DNSSEC. Bao gồm Mô hình triển khai, các bản ghi tài nguyên và các giao thức mở rộng trong DNSSEC. Cụ thể:

* Về các bản ghi tài nguyên DNSSEC: Bảnghi DNSKEY trong một Zone. Bản ghi RRSIG trong một Zone.

Bản ghi chuyển giao DS trong một Zone. Bản ghi NSEC trong một Zone.

Bản ghi NSEC3 trong một Zone.

*Nhận xét:*

Đối với bản ghi tài nguyên CNAME có những thay đổi sau: Khi một tập bản ghi tài nguyên CNAME có ở tên miền trong một Signed Zone, phải có các tập bản ghi tài nguyên RRSIG và NSEC tương ứng ở tên miền đó để giải quyết điểm xung đột trong định nghĩa gốc của bản in CNAME. Đồng thời cho phép một tập bản ghi tài nguyên KEY ở tên miền đó để cập nhật bảo mật động. Các loại khác không được có ở tên miền đó.

Đối với bản ghi tài nguyên DNSSEC xuất hiện ở zone cut: DNSSEC đưa ra hai loại bản ghi tài nguyên mới thường xuất hiện ở phía cha của mặt cắt. Ở phía cha của zone cut (tức là ở điểm chuyển giao), yêu cầu các bản ghi tài nguyên NSEC ở tên miền chủ. Một bản ghi tài nguyên DS cũng có thể có khi zone được chuyển giao này được ký và cố gắng có một chuỗi xác thực đối với zone cha. Điều này là một ngoại lệ đối với tiêu chuẩn DNS gốc, nó quy định rằng chỉ các tập bản ghi tài nguyên NS có thể xuất hiện ở phía cha của zone cut.

Các phần mở rộng trong DNSSEC gồm có:Máy chủ tên miền thẩm quyền.

Máy chủ tên miền đệ quy. Bộ phân giải.

Hỗ trợ xác thực DNS.

# CHƯƠNG 3: ỨNG DỤNG DNSSEC TRONG ĐẢM BẢO AN TOÀN HỆ THỐNG TÊN MIỀN (DNS)

## 3.1. Các phương thức tấn công mạng phổ biến

Hệ thống DNS thực chất là một tập hợp hệ thống phần cứng và các công cụ phần mềm phục vụ cho nhiệm vụ phân giải tên miền.

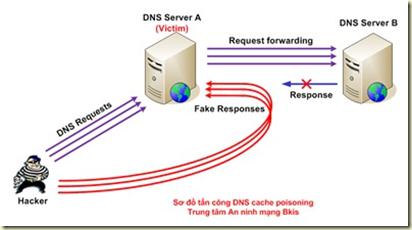
Ngoài các hệ thống phần cứng và các công cụ phần mềm chạy dưới dạng dịch vụ thì cần có các giao thức DNS (Bao gồm định dạng gói tin, giao thức truyền, …) để có thể tiến hành trao đổi thông tin giữa máy client với các máy chủ DNS và giữa các máy chủ DNS với nhau.

Chính vì DNS hội tụ đầy đủ các hệ số: Phần cứng, phần mềm và giao thức như đã trình bày ở trên nên hệ thống DNS luôn luôn tiềm ẩn các lỗ hổng mà hacker có thể sử dụng để khai thác và làm chủ hệ thống, từ đó gây ra các ảnh hưởng tới người dùng.

### **3.1.1. DNS spoofing (DNS cache poisoning)**

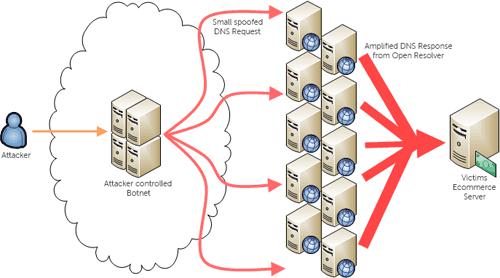
Đây là một phương pháp tấn công máy tính nhờ đó mà dữ liệu được thêm vào hệ thống cache của các DNS máy chủ. Từ đó, các địa chỉ IP sai (thường là các địa chỉ IP do kẻ tấn công chỉ định) được trả về cho các truy vấn tên miền nhằm chuyển hướng người dùng tư một website này sang một website khác.

Để khai thác theo hướng này, kẻ tấn công lợi dụng lỗ hổng của phần mềm DNS, do các hồi đáp DNS không được xác nhận để đảm bảo chúng được gửi từ các máy chủ được xác thực, các bản ghi không đúng đắn sẽ được cache lại và phục vụ cho các user khác.



Ví dụ: Kẻ tấn công thay thế địa chỉ IP cho một bản ghi DNS trên DNS máy chủ thành địa chỉ IP của máy chủ mà kẻ tấn công đang có quyền điều khiển. Trên máy chủ này, kẻ tấn công có triển khai một số phần mềm mã độc để khi người dùng bị chuyển qua sẽ dễ dàng bị nhiễm mã độc.

### **3.1.2. Tấn công khuếch đại dữ liệu DNS (Amplification attack)**

****

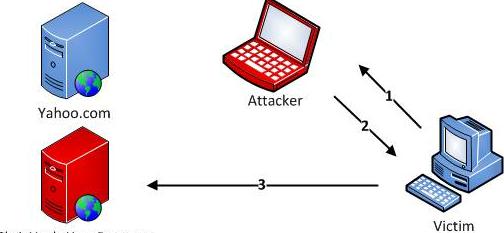
Đây là một trong những phương pháp tấn công được sử dụng để làm nghẽn lưu lượng sử dụng dịch vụ, thuộc vào lớp tấn công ánh xạ.

Có hai yếu tố cơ bản cho cách thức tấn công này:

* Địa chỉ tấn công được che giấu nhờ ánh xạ sang một bên thứ ba.
* Lưu lượng mà người bị hại nhận được sẽ lớn hơn lưu lượng gửi từ kẻ tấn công.

### **3.1.3. Giả mạo máy chủ DNS (Main in the middle)**

Đây là cách một số phần mềm quảng cáo hay trojan thường hay thực hiện. Đầu tiên, chúng dựng lên các DNS máy chủ, giống với chức năng DNS máy chủ thông thường. Tuy nhiên, các DNS máy chủ này có khả năng điều khiển được để thêm, bớt hay chỉnh sửa các bản ghi DNS nhằm chuyển hướng người dùng tới các địa chỉ IP không chính xác với mục đích: gia tăng quảng cáo, cài mã độc, thay đổi kết quả tìm kiếm…



Để thực hiện hành vi này, các phần mềm độc hại sau khi được cài vào máy tính người dùng, chúng sẽ tìm cách để thay đổi cấu hình DNS của người dùng thành địa chỉ DNS của phần mềm đã thiết lập từ trước. Qua đó, các truy vấn DNS của người dùng thay vì đi qua các DNS máy chủ của ISP hoặc do người dùng thiết lập thì lại đi qua các DNS máy chủ của kẻ tấn công.

Một biến thể của hình thức này chính là việc các phần mềm độc hại thay đổi file host (Trên hệ điều hành Windows) để chỉ định địa chỉ IP cho một số website mà kẻ tấn công mong muốn.

Khi tấn công hệ thống DNS, kẻ tấn công mong muốn thực hiện một số hành vi:

* Lừa người sử dụng truy cập tới các website giả mạo do kẻ tấn công lập ra để thực hiện các hành vi lừa đảo, ăn cắp mật khẩu, thông tin đăng nhập, cài cắm các phần mềm độc hại. Các thông tin này có thể vô cùng quan trọng: tài khoản ngân hàng, tài khoản quản trị, …
* Tăng lưu lượng cho website: kẻ tấn công chuyển hướng người dùng khi họ truy cập các website phổ biến về địa chỉ website mà kẻ tấn công muốn tăng lưu lượng. Mỗi khi người dùng truy cập một trong các website kia thì trả về địa chỉ IP website mà kẻ tấn công mong muốn, qua đó làm tăng lưu lượng cho website.
* Gián đoạn dịch vụ: mục đích này nhằm ngăn chặn người dùng sử dụng một dịch vụ của một nhà cung cấp nào đó.

## 3.2. Kịch bản tấn công DNS

Bảo mật an toàn trong DNS là hết sức cần thiết. Microsoft là một trong những nhà cung cấp dịch vụ nhìn nhận vấn đề đó và tiến hành triển khai giao thức DNSSEC giúp tăng tính bảo mật DNS.

Cụ thể Microsoft đã xây dựng kịch bản và quy trình mô phỏng và thử nghiệm

DNSSEC như sau:

Đối với phần trình diễn DNSSEC trong phòng thí nghiệm thử nghiệm, ta có thể sử dụng DNS1 thay vì client1 để thực hiện các truy vấn DNS client, nếu máy tính client1 không có sẵn. Nếu máy tính DC2 là không có sẵn, và ta phải bỏ qua một số thủ tục dưới đây.

Một cuộc thử nghiệm chức năng của DNSSEC trên Windows Server 2012 bao gồm các thủ tục sau đây:

(1). Truy vấn khu vực chưa được đăng nhập mà ko cần xác nhận DNSSEC theo yêu cầu.

(2). Đăng nhập vùng dữ liệu trên DC1 và phân loại anchors (mấu neo) tin cậy.

(3). Truy vấn một khu vực đã đăng nhập mà không cần xác nhận DNSSEC theo yêu cầu.

(4). Truy vấn một khu vực đã đăng nhập cần xác nhận DNSSEC theo yêu cầu.

(5). Không đăng kí vùng dữ liệu sau đó đăng nhập lại vùng với những thông số tùy chỉnh.

(6). Chứng minh (giải thích, thể hiện) xác nhận thất bại.

(7). Chứng minh thư mục hoạt động của DNSSEC đã đăng nhập bản ghi tài nguyên.

(8). Chuyển vai trò Master Key cho sec.contoso.com đến DC2.

* **Cụ thể**

**(1). Truy vấn khu vực chưa được đăng nhập mà ko cần xác nhận DNSSEC theo yêu cầu.**

Đầu tiên, sử dụng resolve-dnsname để truy vấn một vùng ko đăng nhập khi xác nhận ko được yêu cầu.

* Để truy vấn 1 vùng dữ liệu ko đăng nhập mà ko cần xác nhận DNSSEC theo yêu cầu.

Trên Client1, chọn **Windows PowerShell** trên thanh tác vụ, gõ **cd\** và nhấn ENTER.

Bắt đầu chụp 1 Network Monitor nếu muốn. Dừng chụp sau khi ban hành lệnh sau, và sau đó lưu lại sử dụng tên là **Capture1**.

Gõ lệnh sau, và sau đó nhấn **ENTER**:

Rời khỏi màn hình Windows PowerShell để mở các thủ tục sau. - Để xác minh các kết nối từ xa đến dc1.sec.contoso.com

Gõ câu lệnh sau và nhấn **ENTER**:



Nhập mật khẩu cho tài khoản user1 và nhấn **OK**.

Khi bạn được nhắc nhở rằng có một vấn đề với an ninh của máy tính từ xa, chọn **YES**.

Xác minh rằng bạn có thể kết nối thành công với dc1.sec.contoso.com, và sau đó đóng phiên từ xa.

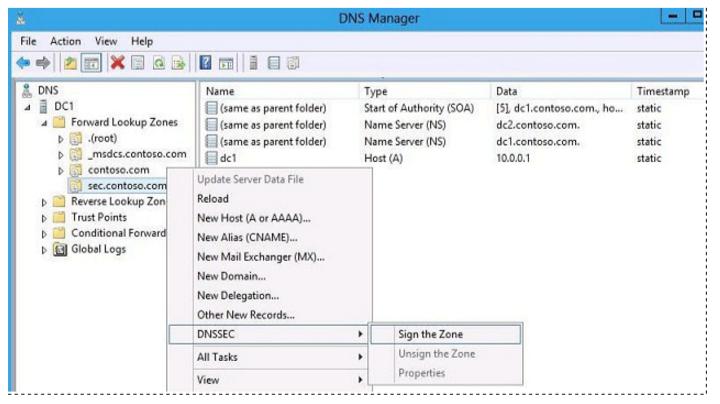
**(2). Đăng nhập vùng dữ liệu trên DC1 và phân phối mấu neo (anchors) tin cậy.**

Tiếp theo, đăng ký vùng sec.contoso.com và phân phối anchor tin cậy cho vùng dữ liệu. Việc phân chia anchor tin cậy là thủ công cho máy chủ DNS mà ko chạy trên vùng của người kiểm soát, như là DNS1. Phân phối các anchor tin cậy tự động có thể được kích hoạt cho máy chủ DNS tích hợp Active Directory như DC2.

* Để đăng ký một zone trên DC1.

Trong bảng điều khiển quản lý DNS trên DC1, di chuyển đến Forward Lookup Zones > sec.contoso.com.

Nhấp chuột phải vào sec.contoso.com trỏ tới DNSSECm và sau đó nhấp vào

**Sign the Zone.**

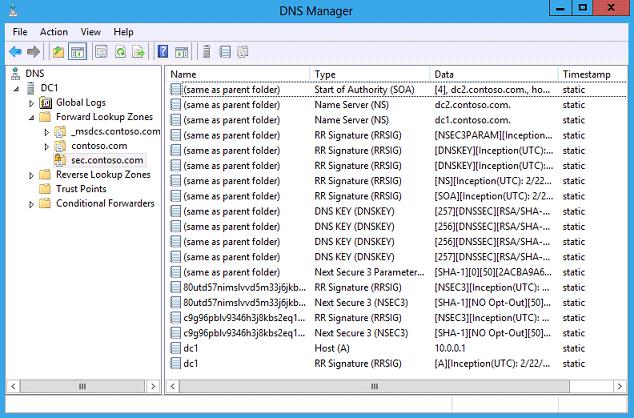
Trong Zone Signing Wizard bấm vào Next, và sau đó chọn Use recommended để cài đặt đăng nhập khu vực.



Bấm vào **Next** hai lần, xác nhận rằng xone đã được đăng ký thành công sẽ được hiển thị, và sau đó nhấp vào **Finish**.

Làm mới giao diện điều khiển trình quản lý DNS và xác minh rằng một biểu tượng mới sẽ được hiển thị cho vùng sec.contoso.com, chỉ ra rằng nó hiện đang được đăng kí với DNSSEC.

Nhấp vào khu vực sec.contoso.com và xem xét các bản ghi tài nguyên mới có mặt, bao gồm cả hồ sơ DNSKEY, RRSIG và NSEC3.

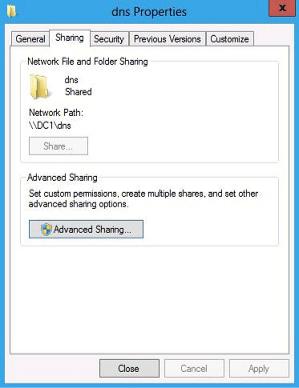


Rời giao diện điều khiển trình quản lý DNS mở. - Để phân phối một anchor tin tưởng đến DNS1

Trên DC1, bấm **Windows Explorer** trên thanh tác vụ.

Điều hướng đến C:\Windows\System32, bấm chuột phải vào thư mục **dns**, chuyển đến **Share with**, và sau đó nhấp vào **Advanced sharing**.

Trong hộp thoại **dns Properties** nhấp vào **Advanced Sharing**, chọn chia sẻ thư mục hộp kiểm này, kiểm chứng **Share name** là **dns** và sau đó nhấp vào **OK.**

****

Nhấp vào **Close** và sau đó đóng Windows Explorer.

Trên DNS1, trong cây bảng điều khiển quản lý DNS, điều hướng đến thư mục

**Trust Points.**

Nhấp chuột phải vào **Trust Points,** trỏ vào **Import,** và sau đó nhấp vào

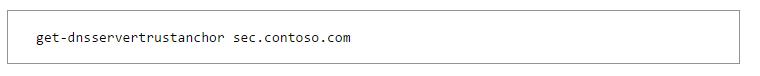
**DNSKEY.**

Trong hộp thoại **Import DNSKEY,** nhập [\\dc1\dns\keyset-sec.contoso.com](https://ssl.microsofttranslator.com/bv.aspx?from=&to=vi&a=%5C%5Cdc1%5Cdns%5Ckeyset-sec.contoso.com) và sau đó nhấp vào **OK**.

* Để xác minh những Anchor tin cậy

Trong cây giao diện điều khiển, điều hướng đến **Trust Points > com >** **contsoso > sec** và xác minh rằng chuyển nhập đã thành công.

Trên bất kỳ máy tính nào, bấm vào **Windows PowerShell**, gõ các lệnh sau đây và sau đó nhấn **ENTER**:



Xác minh rằng hai anchor tin cậy được hiển thị.

Trên DNS1, bấm chuột phải vào **Windows PowerShell** và sau đó nhấp vào **Run as Administrator.**

Gõ câu lệnh sau và nhấn Enter:

Xác minh rằng hai anchor tin cậy được hiển thị.



* Xóa và tái phân phối anchor tin cậy trên Windows PowerShell

Trên DNS1, trong cửa sổ Administrator Windows PowerShell, gõ lệnh dưới đây và nhấn **ENTER** hai lần.

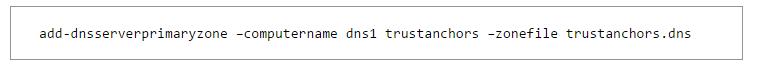
Gõ câu lệnh sau và nhấn Enter



(Xác minh rằng “Không thể liệt kê các anchor tin cậy" sẽ được hiển thị.)

Gõ câu lệnh sau và nhấn **Enter** hai lần.

Gõ câu lệnh sau và nhấn **Enter**.



*Gõ câu lệnh sau và nhấn Enter*

get-dnsserverresourcerecord –zonename sec.contoso.com –rrtype dnskey – computername dc1 | %{ $\_.recorddata

Gõ câu lệnh sau và nhấn **Enter**.

get-dnsserverresourcerecord – zonename sec.contoso.com –rrtype dnskey – computername dc1 | %{ $\_.recorddata

Gõ câu lệnh sau và nhấn **Enter**.

Xác minh rằng hai anchor tin cậy một lần nữa được hiển thị.



* Để phân phối achor tin cậy đếnDC2

Trên DC1, trong cây giao diện điều khiển quản lý DNS, di chuyển về

**To Forward Lookup Zones** > **sec.contoso.com**.

Nhấp chuột phải vào **sec.contoso.com**, trỏ tới **DNSSEC**, và sau đó nhấp vào

**Properties.**

Nhấp vào **Trust Anchor**

Chọn **Enable the distribution of trust anchors for this zone** sau đó nhấn **OK**. *Khi bạn được nhắc xác nhận thay đổi vùng, bấm Yes*

Khi được nhắc xác nhận thay đổi vùng, bấm **YES**.

Khi được nhắc rằng việc nhập cấu hình đó đã thành công, bấm vào **OK**.

Trên DC2, làm mới giao diện trong trình quản lý DNS và xác nhận rằng anchor tin cậy cho **sec.contoso.com** đang có mặt.

**(3). Truy vấn một vùng được đăng kí mà không cần xác nhận của DNSSEC:**

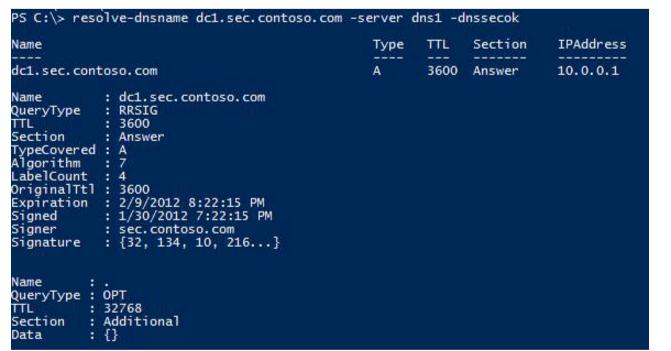
Bổ sung thông tin liên quan DNSSEC được hiển thị cho các hồ sơ tài nguyên đã ký kết. So sánh kết quả truy vấn cho dc1.contoso.com để truy vấn kết quả cho dc1.sec.contoso.com nếu muốn.

* Truy vấn một vùng được đăng kí mà không cần xác nhận của DNSSEC.

Bắt đầu chụp một Network Monitor nếu muốn. Dừng chụp sau khi đưa ra lệnh và sau đó lưu lại dưới tên **Capture2**.

Trên Client1, tại màn hình Windows PowerShell gõ lệnh sau đây và sau đó nhấn **Enter**.



Màn hình hiển thị

Để xác minh rằng DNSSEC hiện tại không được yêu cầu, gõ lệnh sau và nhấn

**ENTER**:

Xác nhận rằng không có chính sách NRPT cho namespace sec.contoso hiện đang áp dụng cho các máy client (máy tính của khách hàng).

Rời khỏi màn hình Windows PowerShell mở.

**(4). Truy vấn một vùng được đăng kí với chứng nhận DNSSEC cần:**

The Name Resolution Policy Table (NRPT) được sử dụng để yêu cầu xác nhận DNSSEC. NRPT có thể được cấu hình trong Group Policy cho một máy tính duy nhất, hoặc Group Policy chính cho một số hoặc tất cả các máy tính trong miền. Quy trình sau sử dụng tên miền Group Policy.

* Yêu cầu DNSSEC xác nhận được thực hiện:

Trên DC1, trên thanh công cụ quản lý máy chủ, nhấn **Tools**, và sau đó nhấp vào

**Group Policy Managenment.**

Trong bảng cây điều khiển Group Policy, dưới **Domains** > **contoso**.**com** > **Group Policy Objects**, và nhấp chuột phải vào **Defaul Domain Policy**, vàochọn **Edit**.

Trong bảng cây điều khiển quản lý Group Policy, điều hướng đến **Computer** **Configuration** > **Policies** > **Windows Settings** > **Name Resolution Policy**.

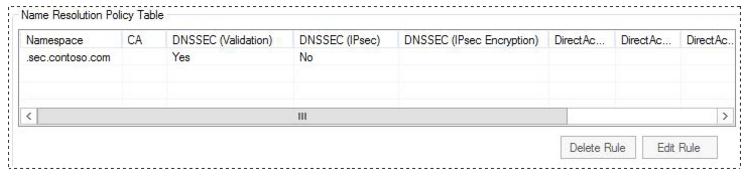
Trong cửa sổ chi tiết, dưới **Create Rules** không áp dụng quy tắc này. Chọn **Suffix** sec.contoso.com bên cạnh **Suffix**.

và đó là một phần của **namespace** từ danh sách thả xuống và nhập

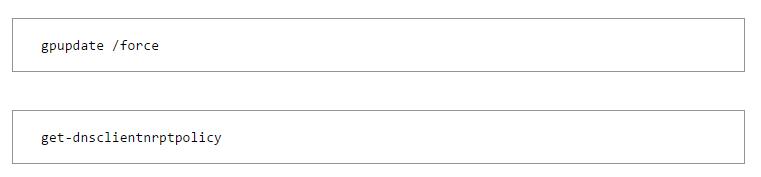
Trên tab **DNSSEC**, chọn **kích hoạt DNSSEC trong quy tắc này** trong hộp kiểm tra và sau đó theo **Validation** chọn **Yêu cầu khách hàng DNS** để kiểm tra xem tên và địa chỉ dữ liệu đã được xác nhận bởi các hộp kiểm máy chủ DNS.

Ở góc dưới bên phải, nhấp vào **Create** và sau đó xác nhận rằng một quy tắc cho sec.contoso.com đã được bổ sung trong phần **Name Resolution Policy**.

Bấm **Apply**, sau đó đóng **Group Policy Management Editor** (các trình soạn thảo chính sách Nhóm quản lý)

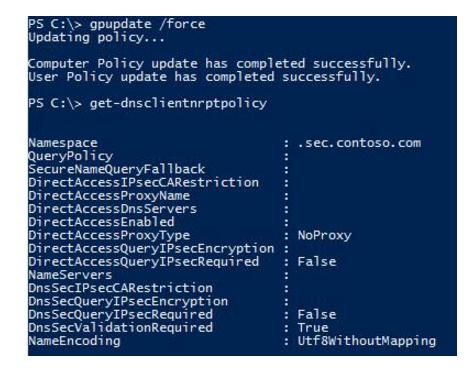


DC1, gõ các lệnh sau dấu nhắc Windows PowerShell, và sau đó nhấn **ENTER**.



Xác minh rằng máy tính và người dùng chính sách thông tin cập nhật thành công, và giá trị của **DnsSecValidationRequires** là đúng cho những namespace của sec.contoso.com

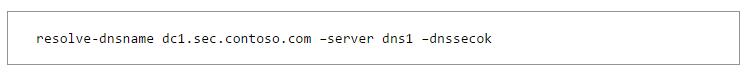
Lặp lại các bản Group Policy (Cập Nhật chính sách Nhóm) (Gpupdate/force) và xác minh NRPT chính sách về client1.



* Truy vấn vùng được đăng kí với DNSSEC xác nhận yêu cầu

Bắt đầu chụp màn hình mạng nếu muốn. Ngừng chụp sau khi phát hành các lệnh sau đây, và sau đó lưu chụp bằng cách sử dụng tên: **Capture3**.

Ở client1, tại dấu nhắc Windows PowerShell, gõ các lệnh sau đây và sau đó nhấn ENTER.



Xác nhận rằng các kết quả tương tự được trả về như trước đây trước khi xác nhận được yêu cầu. Bởi vì một anchor tin tưởng có giá trị có mặt trên DNS1, truy vấn thành công ngay cả khi xác nhận được yêu cầu.

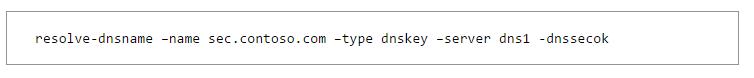
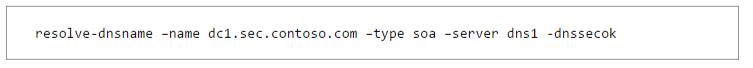
**Truy vấn DNSSEC records trong vùng sec.contoso.com.zone**

Trước khi bỏ đăng kí và tái đăng ký khu vực, đưa ra một số truy vấn cho bản ghi DNSSEC. Những loại truy vấn này có thể hữu ích khi giải đáp thắc mắc DNSSEC.

* Để truy vấn DNSSEC records ở khu vực [sec.contoso.com](https://ssl.microsofttranslator.com/bv.aspx?from=&to=vi&a=sec.contoso.com)

Ở client1, tại dấu nhắc Windows PowerShell, gõ các lệnh sau đây và sau đó nhấn **ENTER**.

Ở client1, tại dấu nhắc Windows PowerShell, gõ các lệnh sau đây và sau đó nhấn **ENTER**.



**(5) Bỏ đăng kí khu vực và sau đó tái đăng vùng với tùy chỉnh các thông số**

DNSSEC ký sẽ được gỡ bỏ từ vùng sec.contoso.com và sau đó khu vực sẽ được tái ký hợp đồng bằng cách sử dụng tùy chỉnh các thông số DNSSEC.

* Để bỏ đăng kí các khu

Trên DC1, trong cây bảng điều khiển quản lý DNS, điều hướng đến **Forward**

**Lookup Zones > sec.contoso.com**

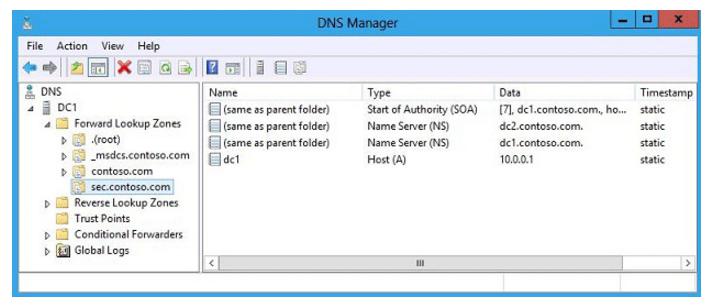
Nhấp chuột phải chọn **sec.contoso.com,** trỏ đến **DNSSEC**, và sau đó chọn

**Unsign the Zone**

Trong wizard của Unsign chọn **Next**.

Kiểm chứng rằng vùng đã được bỏ đánh dấu thành công sẽ được hiển thị, và sau đó nhấp vào **Finish**.

Làm mới giao diện trong trình quản lý DNS và xác minh rằng vùng **sec.contoso.com** không còn chứa DNSSEC signed records, và biểu tượng bêncạnh khu vực chỉ ra nó không được đăng ký.



* Tái đăng ký vùng với tùy chỉnh các thông số

Tại DC1, nhấn chuột phải vào **sec.contoso.com,** chọn đến **DNSSEC**, và sau đó chọn **Sign the Zone.**

Tại vùng **Zone Signing Wizard,** nhấp vào **Next.**

Tùy chỉnh vùng đăng nhập tham số được chọn theo mặc định. Bấm vào **Next**.

Trên trang Key Master, DNS server DC1 là một khóa quan trọng được chọn đặt mặc định, vì vùng đăng kí đang được thực hiện trên DC1.

Nếu bạn đã cấu hình DC2 trong phòng thí nghiệm thử nghiệm này, xem xét tùy chọn có sẵn khi **Select another primary server as the Key Master.** Không chọn tùy chọn này, nhưng xác minh rằng dc2.contoso.com này cũng có sẵn như là một khóa chủ thể cho vùng này. Khi bạn được cảnh báo rằng tất cả các máy chủ ủy quyền có khả năng đăng nhập trực tuyến DNSSEC sẽ được nạp, bấm **YES**.



Đảm bảo rằng DC1 lựa chọn làm chủ quan trọng và sau đó nhấp vào Next hai lần.

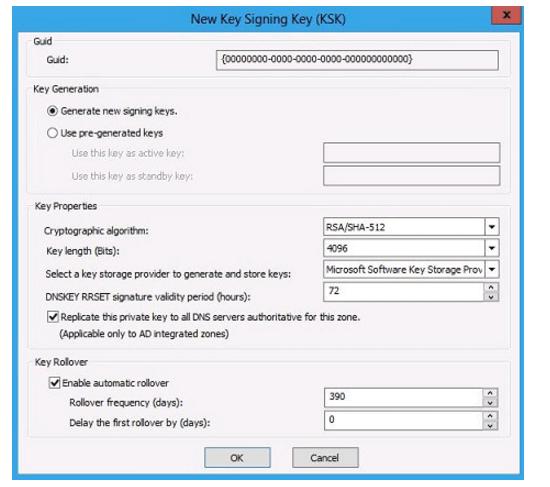
Trong các phím **Key Signing (KSK),** trang, bấm hiện KSK (với phím dài 2048), và sau đó nhấn vào **Remove**.

Để thêm một KSK, bấm vào **Add**

Trong hộp thoại mới **New Key Signing Key (KSK),** dưới **Key Ptoperties**, hãy nhấp vào phần thả xuống bên cạnh các **Cryptographic algorithm** và lựa chọn

**RSA/SHA – 512.**

Theo **Key Properties**, nhấp vào phần thả xuống bên cạnh **Key length** (**Bits**) và lựa chọn **4096** rồi sau đó nhấp vào **OK**.



Nhấp vào **NEXT** cho đến khi hiện thông báo **You have successfully** **configured the following parameters to sign the zone** trên màn hình

Xem lại các tham số bạn đã lựa chọn và sau đó bấm **Next** để bắt đầu quá trình đăng kí vùng.

Xác nhận rằng **The zone has been successfully signed** trên màn hình, nhấp vào Finish, và sau đó làm mới giao diện trong trình quản lý DNS để xác minh vùng đó được đăng kí lần nữa.

Làm mới chế độ xem cho thư mục **Trust Points** và kiểm chứng rằng điểm mới tin tưởng DNSKEY sử dụng thuật toán RSA/SHA – 512.

Một lời nhắc người quản trị Windows PowerShell, gõ các lệnh sau và nhấn

**Enter**.

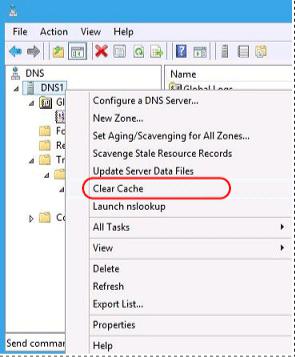
**(6) Chứng minh xác nhận không thành công**

Bởi vì các anchor tin cậy được phân phối đến các DNS1 không còn hợp lệ, DNSSEC xác nhận sẽ thất bại khi bản ghi tài nguyên được truy vấn trong khu vực sec.contoso.com.

* Để chứng minh thất bại trong việc xác nhận

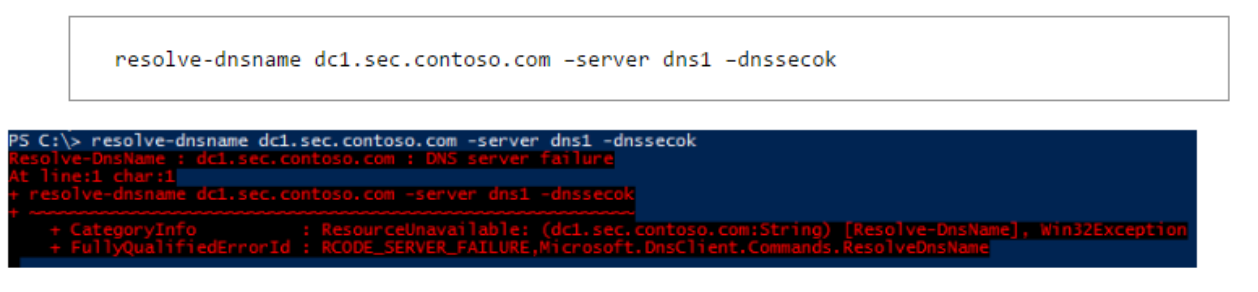
Trên DNS1, xem cài đặt gần đây **Trust Points** cho [sec.contoso.com](https://ssl.microsofttranslator.com/bv.aspx?from=&to=vi&a=sec.contoso.com) và xác minh anchor tin cậy cũ sử dụng thuật toán RSA/SHA-1 được trình bày.

Để làm sạch bộ nhớ cache DNS server, bấm chuột phải vào DNS1 và sau đó nhấp vào Clear Cache.



Bắt đầu một Network Monitor nếu muốn. Ngừng chụp sau khi cấp các lệnh sau đây, và sau đó lưu chụp bằng cách sử dụng tên: **Capture4**.

Trên client1, gõ lệnh sau tại dấu nhắc Windows PowerShell và sau đó nhấn **ENTER.**



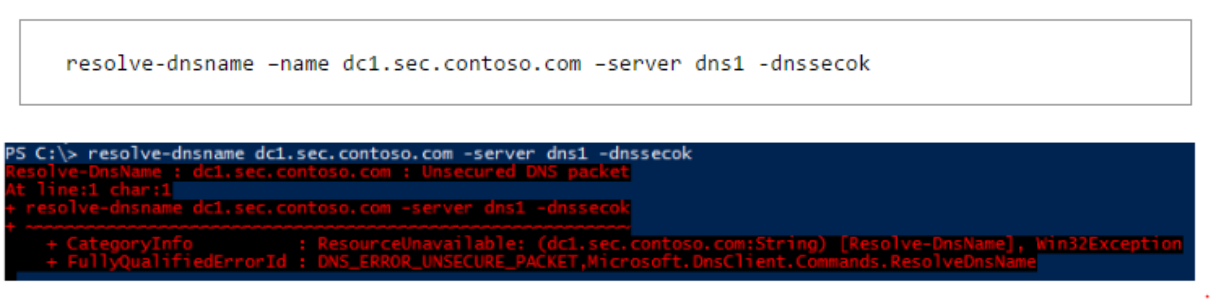
**Note:**

Tự động cập nhật của anchor tin cậy vào một các máy chủ DNS (mỗi RFC 5011) không ủy quyền, phê chuẩn chỉ xảy ra trong quá trình tái đầu tư quan trọng. Nếu bạn không đăng ký và tái đăng kí khu vực một cách thủ công với phím mới, bạn cũng bắt buộc phải phát hành một anchor tin tưởng mới theo cách thủ công. Nếu một máy chủ DNS validating có một anchor tin cậy không chính xác, truy vấn DNS yêu cầu xác nhận sẽ chỉ ra một máy chủ thất bại. Khi không có anchor tin cậy được trình bày, truy vấn cũng thất bại trong việc xác nhận. Kể từ khi không có anchor tin cậy, các máy chủ không tìm cách để xác nhận các phản ứng. Trong trường hợp này, một lỗi gói ko bảo đảm sẽ được hiển thị.

* **Để chứng minh một phản ứng unsecure**

Trên DNS1, tại Administrator Windows PowerShell, gõ các lệnh sau đây và sau đó nhấn **ENTER** hai lần:

Bắt đầu chụp Network Monitor nếu muốn. Ngừng chụp sau khi phát.

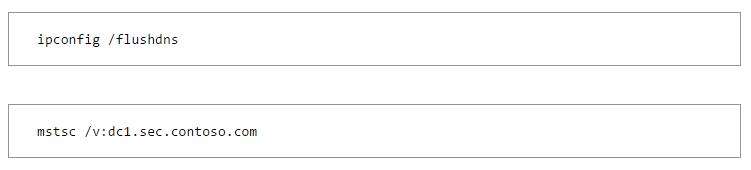
hành các lệnh sau đây, và sau đó lưu chụp bằng cách sử dụng tên: **Capture5**. Gõ lệnh sau và nhấn **ENTER**:

**Chứng minh sự thất bại của máy tính để bàn từ xa.**

Bởi vì DNSSEC xác nhận không thành công, bạn không thể kết nối đến dc1.sec.contoso.com bằng cách sử dụng máy tính để bàn từ xa.

* Để chứng minh sự thất bại của máy tính để bàn từ xa

Trên client1, gõ lệnh sau tại dấu nhắc Windows PowerShell và sau đó nhấn **ENTER**



Xác minh rằng máy tính để bàn từ xa không thể tìm thấy máy tính “dc1.sec.contoso.com” sẽ được hiển thị.

1. **Chứng minh thư mục hoạt động sao chép của DNSSEC đăng ký bản ghi tài nguyên.**

Khi máy chủ DNS được tích hợp Active Directory, anchor tin cậy và bản ghi tài nguyên được kí kết được cập nhật tự động ngay cả khi khu vực ko đăng kí và tái đăng nhập theo cách thủ công.

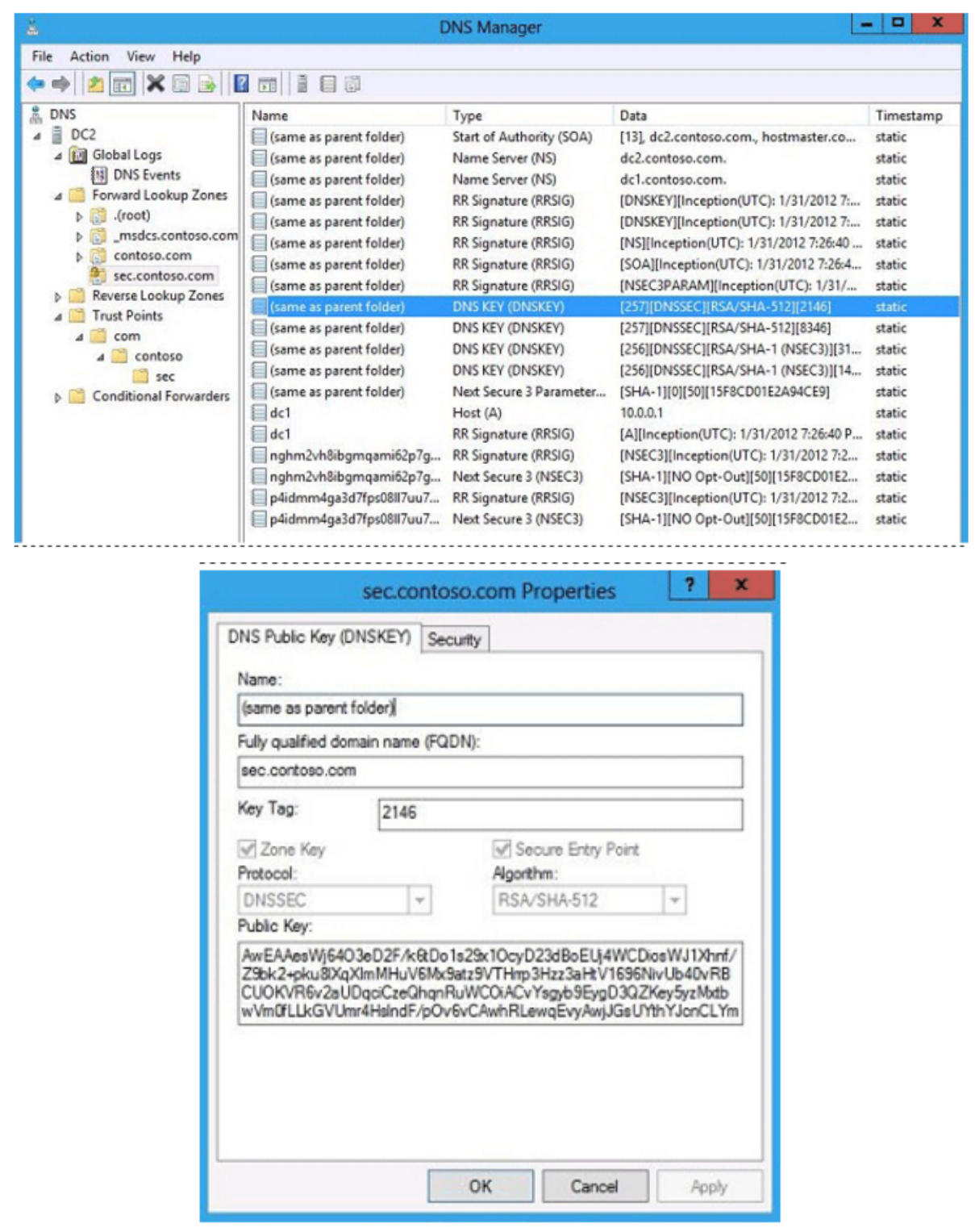
* Để chứng minh hoạt động thư mục sao chép DNSSEC ký kết bản ghi tài nguyên.

Trên DC2, trong trình quản lý DNS, xem nội dung của thư mục Trust Points . Làm mới giao diện nếu cần thiết để xem các anchor tin cậy hiện nay.

Xác minh rằng anchor tin cậy DNSKEY cho sec.contoso.com tự động Cập Nhật để sử dụng thuật toán RSA/SHA-512.

Trong bảng điều khiển quản lý DNS, nhấp vào Global Logs > DNS Events và xem xét tổ chức sự kiện ID 7653 mà chỉ ra rằng các máy chủ DNS đã phát hiện ra rằng khu ký các tham số cho các khu vực sec.contoso.com đã được thay đổi và khu vực sẽ được tái ký. Trường hợp không có sẽ được hiển thị sau khi khu vực ký xong.

Nhấn vào **Forward Lookup Zones > sec.contoso.com** trong giao diện điều khiển cây mà xác minh Secure Entry Point DNSKEY đươc trình bày sử dụng thuật toán RSA/SHA-512.



Trên DC1, trong trình quản lý DNS, thêm bản ghi lưu trữ (A) mới cho dns1.sec.contoso.com với địa chỉ IP của 10.0.0.2.

Trên DNS1, xem cài đặt gần đây Trust Points cho sec.contoso.com và xác minh anchor tin cậy cũ sử dụng thuật toán RSA/SHA-1 được trình bày.

Trên DC2, làm mới giao diện trong trình quản lý DNS và xác minh hồ sơ ký mới đã nhân rộng đến máy chủ này.

1. **Để Chuyển vai trò chủ quan trọng cho** [**sec.contoso.com**](https://ssl.microsofttranslator.com/bv.aspx?from=&to=vi&a=sec.contoso.com) **sang DC2**

Trên DC1 hoặc DC2, trong trình quản lý DNS, nhấp chuột phải vào vùng sec.contoso.com trỏ tới DNSSEC, và sau đó nhấp vào **Properties**.

Trên tab Key Master, hãy chọn Use the following DNS server as the Key Master.

Nhấp vào danh sách thả xuống và khi bạn đang cảnh báo tất cả các máy chủ DNS uỷ quyền sẽ được nạp, bấm **Yes.**

Chọn **dc2.contoso.com** từ danh sách và sau đó nhấp vào **OK**.

Khi bạn được cảnh báo rằng chủ quan trọng sẽ thay đổi thiết đặt, bấm **Yes**

Xác minh rằng chủ quan trọng cho sec.contoso.com khu vực được cập nhật thành công sẽ được hiển thị.

Kiểm tra DNS tổ chức sự kiện ID 7649 sẽ được hiển thị trên Key Master và DNS sự kiện mới ID 7648 sẽ được hiển thị trên chủ quan trọng trước đó.

## 3.3. Giải pháp DNSSEC đối với kịch bản tấn công DNS

Một cuộc tấn công khuếch đại lưu lượng dữ liệu trong DNS (hay còn gọi là tấn công ánh xạ DNS) là một loại tấn công từ chối dịch vụ (Ddos) bằng cách lợi dụng một DNS nhỏ để có thể tạo ra tạo ra một phản hồi lớn. Khi kết hợp với địa chỉ giả mạo, kẻ tấn công có thể nhắm vào một lượng lớn lưu lượng mạng đến hệ thống mục tiêu bằng cách khởi tạo các truy vấn DNS nhỏ.

Các yếu tố khuếch đại trong kiểu tấn công này phụ thuộc vào loại truy vấn DNS và có máy chủ DNS hay không (sử dụng như một tấn công trung gian) hỗ trợ việc gửi các gói tin UDP lớn trong cuộc tấn công đó. Đây là tính năng nhằm tối ưu hóa thông tin DNS. Nếu một máy chủ DNS không hỗ trợ dung lượng lớn (> 512 byte) các gói tin UDP trong một phản hồi, nó có thể quay lại TCP. Điều này làm giảm hiệu quả của một cuộc tấn công khuếch đại bởi vì TCP ít bị giả mạo địa chỉ.

Một kẻ tấn công đang có kế hoạch tấn công DNS mở rộng có thể lợi dụng những điều sau đây:

Mở đệ quy: Tên miền trên Internet đã kích hoạt đệ quy và cung cấp DNS đệ quy phản hồi cho bất cứ ai, được gọi là "phân giải mở". Số lượng máy chủ DNS cung cấp đệ quy mở trên Internet đã được ước tính từ vài trăm ngàn đến vài triệu. Trong một cuộc tấn công DNS mở rộng, các chức năng mở của thiết bị giải là nguồn gốc của sự khuếch đại, tiếp nhận một truy vấn DNS nhỏ và trả lại một phản hồi DNS hoàn toàn lớn hơn nhiều. Các máy chủ DNS thường không bị tổn hại, thực tế lại hoạt động như bình thường.

* Địa chỉ nguồn giả mạo: Địa chỉ nguồn giả mạo làm thay đổi địa chỉ trả về một gói tin để giả định các gói tin đến từ một nguồn nào khác ngoài người gửi. Trong một cuộc tấn công khuếch đại DNS, địa chỉ nguồn cho các truy vấn giả mạo DNS cùng mục tiêu tấn công, tương tự như cuộc tấn công "Smurf". Khi bộ phân giải trả về một DNS phản hồi, phản hồi này là không chính xác và được gửi từ địa chỉ giả mạo.
* Botnet: Botnet là nhóm máy tính trực tuyến đã bị xâm nhập bởi một kẻ tấn công. Botnet được sử dụng trong một cuộc tấn công DNS mở rộng để gửi truy vấn DNS tới bộ phân giải mở.
* Malware: Malware có thể được sử dụng để truy cập vào máy tính botnet và cung cấp phương tiện để gây ra cuộc tấn công DNS mở rộng.
* EDNS0: Mở rộng cơ chế cho DNS cho phép DNS requestor quảng cáo kích thước của gói tin UDP và tạo thuận lợi cho việc chuyển các gói tin lớn hơn 512 byte. Nếu không có EDNS0, một truy vấn 64 byte có thể đưa kết quả (ít nhất) tại 512 byte UDP phản hồi tương ứng với hệ số khuếch đại 512/64 = 8.
* DNSSEC: DNSSEC thêm bảo mật cho các phản hồi DNS bằng cách cung cấp khả năng cho các máy chủ DNS xác nhận câu trả lời DNS. DNSSEC ngăn chặn các cuộc tấn công mã độc bộ nhớ cache, nhưng bổ sung thêm chữ ký mật mã nên thông điệp DNS có dung lượng lớn hơn. Mặt khác, DNSSEC cũng yêu cầu EDNS0 hỗ trợ; do đó máy chủ hỗ trợ DNSSEC đồng thời hỗ trợ các gói tin UDP lớn trong phản hồi DNS.

Nếu mục tiêu của cuộc tấn công là máy chủ DNS, cuộc tấn công DNS mở rộng sử dụng các truy vấn cho một zone DNSSEC ký có tiềm năng để tăng việc sử dụng bộ vi xử lý do việc mã hóa liên quan đến việc DNSSEC chứng thực đã đăng nhập vào dữ liệu tài nguyên. Các máy chủ DNS chỉ cần bỏ qua các gói tin. Lưu ý: Máy chủ DNS chạy Windows gửi các gói dữ liệu và đăng nhập trong thực hiện và thống kê truy cập theo loại gói tin của phản hồi chưa khớp.

Điều quan trọng cần lưu ý là bản thân DNSSEC không cho phép một cuộc tấn công DNS mở rộng thành công. Như đã nêu trước đó, một yếu tố khuếch đại có thể không có EDNS0 hoặc DNSSEC. Các cuộc tấn công DNS mở rộng thành công không đòi hỏi EDNS0 hoặc DNSSEC.

Để chứng minh một cuộc tấn công mở rộng hoạt động như thế nào, và làm sao nó bị ảnh hưởng bởi DNSSEC, giả định rằng một bản ghi TXT rất lớn đã được tạo ra trên một máy chủ DNS. Lưu ý rằng, nếu dữ liệu là quá lớn, các máy chủ sẽ không sử dụng UDP thậm chí nếu EDNS0 được kích hoạt. Theo mặc định, một máy chủ DNS đang

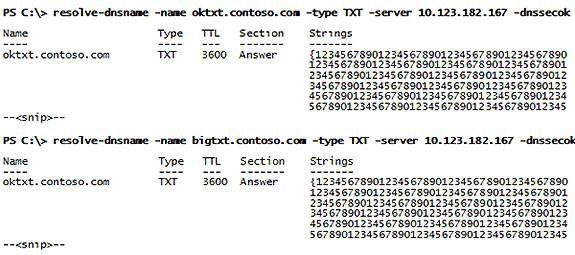
chạy Windows sẽ rơi trở lại TCP cho những hồ sơ lớn hơn 4000 byte. Điều này có thể được chứng minh bằng một thiết bị giám sát mạng:

Trong ví dụ sau, hai bản ghi TXT được tạo ra trên một máy chủ DNS chạy Windows Server 2012 tại 10.123.182.167. Mỗi dữ liệu TXT bao gồm các dòng văn bản dài 256 byte.

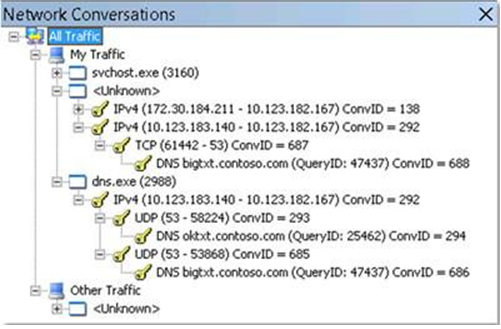
Tên miền oktxt.contoso.com chứa 15 dòng: 15 x 256 = 3840 bytes.

Tên miền bigtxt.contoso.com chứa 16 dòng: 16 x 256 = 4096 bytes.

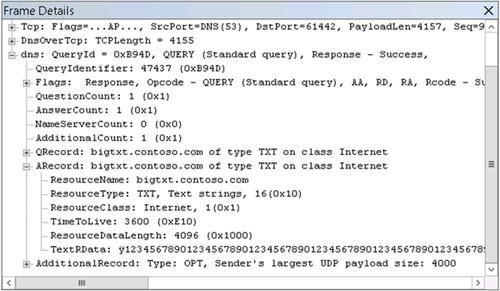
Cung cấp một truy vấn cho các dữ liệu và xác định rằng các gói tin UDP lớn được cho phép trong các phản hồi, chúng ta có thể sử dụng dig (dig @10.123.182.167 oktxt.contoso.com any +edns=0) hoặc resolve-dnsname Windows PowerShell cmdlet có sẵn trong Windows Server 2012. dnssecok flag cho máy chủ mà gói tin phản hồi UDP lớn được hỗ trợ:



Các truy vấn trên được đưa ra từ một máy tính khách hàng tại 10.123.183.140. Thiết bị giám sát mạng trên máy chủ DNS cho thấy tên miền bigtxt.contoso.com sử dụng TCP trong khi oktxt.contoso.com sử dụng UDP:



Cụ thể, các chi tiết frame cho các truy vấn này cho thấy kích thước UDP playload lớn nhất là 4000 byte, và trong trường hợp của dữ liệu bigtxt.contoso.com kích thước là 4.096 byte (vượt quá giới hạn):

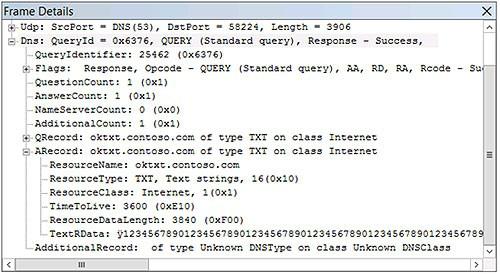


Khi 4000 byte UDP giới hạn bị vượt quá, các máy chủ DNS sử dụng TCP trong phản hồi DNS.

Giới hạn 4000 byte cũng có thể hiển thị trên máy chủ DNS sử dụng Windows PowerShell:

PS C:\> (Get-DnsServer).ServerSetting.MaximumUdpPacketSize 4000

Các chi tiết trong frame cho tên miền oktxt.contoso.com biểu diễn trong bảng dưới. Chỉ UDP được sử dụng cho các dữ liệu tài nguyên có chiều dài 3840 byte vì nó dưới giới hạn 4000 byte:



Nhắc lại rằng UDP là quan trọng trong các cuộc tấn công DNS mở rộng vì địa chỉ nguồn giả mạo là một phần quan trọng của cuộc tấn công. Cách bắt tay ba (three- way handshake) được sử dụng bởi TCP làm việc giả mạo khó khăn hơn khi DNS phản hồi sử dụng UDP. Do đó, kẻ tấn công thường muốn giới hạn kích thước của phản hồi để chỉ UDP được sử dụng.

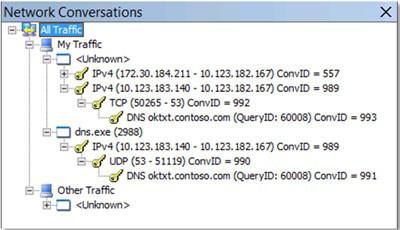
Một kẻ tấn công sử dụng các dữ liệu TXT oktxt.contoso.com về mặt lý thuyết có thể sử dụng kích thước đơn vị truyền tối thiểu là 64 byte để phát hành một truy vấn mà trả về một phản hồi UDP 3840 byte, cho hệ số khuếch đại 3840/64 = 60.

* DNS phản hồi trong miền được ký

Điều gì xảy ra nếu miền được ký? Windows Server 2012 hỗ trợ vùng sử dụng Windows PowerShell hoặc sử dụng miền DNSSEC có sẵn trong bộ quản lý DNS. Quá trình này cho thêm một số dữ liệu tài nguyên mới vào khu vực, và những dữ liệu này được trả về với kết quả truy vấn. Điều này có làm tăng hệ số khuếch đại trong một cuộc tấn công DNS mở rộng không?

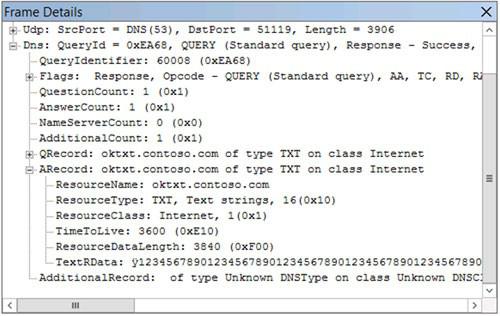
Sau khi miền được ký, một truy vấn cho tên miền oktxt.contoso.com (bản ghi

TXT nhỏ hơn) cung cấp sự kết hợp sau:



Có một sự kết hợp TCP ngoài UDP, tương tự như những gì đã xảy ra trước đây với các dữ liệu TXT lớn trong tên miền bigtxt.contoso.com.

Kiểm tra các chi tiết frame cho việc trao đổi UDP cho thấy các bản ghi TXT cũng được gửi qua UDP như đã được gửi trước khi miền được ký:



Sau khi miền được ký, các gói trao đổi TCP bao gồm các dữ liệu liên quan

DNSSEC (RRSIG):



Việc đăng ký miền DNS và thêm các dữ liệu DNSSEC tới một DNS phản hồi tăng tổng kích thước của một phản hồi, nhưng không làm tăng nguy cơ bị mở rộng DNS qua giới hạn hiện tại được đặt trên máy chủ cho kích thước phản hồi UDP.

Từ khi sự kết hợp của TCP không dễ bị giả mạo, những dữ liệu bổ sung không làm tăng mức độ nghiêm trọng của các cuộc tấn công DNS mở rộng.

Tuy nhiên, hệ số khuếch đại 60 lần là không hề nhỏ, và các cuộc tấn công DNS mở rộng tiếp tục là một nguy cơ trên Internet. Một số điều bạn có thể làm để ngăn chặn các cuộc tấn công khuếch đại DNS bao gồm:

* Không đặt DNS mở trên Internet. Hạn chế khách hàng truy cập được vào bộ giải làm giảm đáng kể khả năng kẻ tấn công sử dụng nó. Điều này có thể được thực hiện bằng các quy tắc firewall, danh sách truy cập router IP, hoặc các phương pháp khác.
* Ngăn chặn địa chỉ IP giả mạo bằng các cấu hình Unicast Reverse Path Forwarding (URPF) trên các router mạng. Một router có cấu hình sử dụng URPF hạn chế khả năng kẻ tấn công giả mạo gói tin bằng cách so sánh địa chỉ nguồn của gói tin với bảng định tuyến nội bộ để xác định địa chỉ là chính đáng. Nếu không, các gói tin bị loại bỏ.
* Triển khai thiết bị hệ thống phòng chống xâm nhập (IPS) hoặc giám sát giao thông DNSSEC. Một số lượng lớn các gói tin gửi đi với cùng một địa chỉ, đặc biệt đột nhiên tăng vọt, là chỉ số tốt cho cuộc tấn công tích cực. Triển khai các bộ lọc để thả, giới hạn, hoặc trì hoãn các tệp nghi ngờ để giảm bớt tác động của các cuộc tấn công trên mạng và tấn công mục tiêu địa phương. Như đã đề cập trước đó, Windows DNS server 2012 gửi gói tin phản hồi chưa khớp và đăng nhập chúng trong giải quyết và thống kê counter. Điều quan trọng là phải thường xuyên theo dõi giám sát lưu lượng.

## 3.4. Kết luận

Chương 3 đưa ra các mô hình tấn công mạng và các đặc điểm của chúng. Tấn công mã độc DNS, tấn công khuếch đại dữ liệu DNS và giả mạo máy chủ DNS. Cùng với đó là kịch bản mô hình tấn công và giải pháp DNSSEC trên máy chủ Windows server 2012 của Microsoft. Đó cũng là ví dụ thực tiễn về hiệu quả và an toàn khi áp dụng giải pháp bảo mật DNSSEC cho hệ thống tên miền DNS.

# KẾT LUẬN

Hệ thống tên miền và hệ thống máy chủ tên miền chính là lỗ hổng lớn của Internet. Hacker có thể lợi dụng lỗ hổng này để thực hiện các mục đích xấu như ăn cắp thông tin, lừa đảo, giả mạo. Do đó cần chú trọng vào bảo mật hệ thống tên miền DNS và một trong những phương pháp được lựa chọn áp dụng là DNSSEC - ứng dụng bảo mật tên miền.

Sau gần hai tháng tìm hiểu, nghiên cứu về ứng dụng bảo mật hệ thống tên miền DNSSEC em đã có thêm nhiều kiến thức mới thật bổ ích trong lĩnh vực an toàn thông tin mạng, đó là một phần trong hành trang quý báu cho em sau này trên con đường lĩnh hội tri thức. Bên cạnh đó khả năng tìm tòi, học hỏi và tư duy của em cũng được hoàn thiện và nâng cao. Tuy nhiên, do kiến thức còn hạn chế nên trong đề tài này sẽ khó tránh khỏi sai sót. Rất mong nhận được ý kiến đóng góp từ quý thầy cô và mọi người.

Đồ án đã đưa ra các nội dung:

* Nghiên cứu về hệ thống tên miền DNS, giới thiệu về DNSSEC.
* Tình hình triển khai và tiêu chuẩn hóa trên thế giới và tại Việt Nam.
* Nghiên cứu về mô hình triển khai, các bản tin tài nguyên, và các giao thức mở rộng trong DNSSEC.
* Ứng dụng DNSSEC trong đảm bảo an toàn hệ thống tên miền DNS. Với các kịch bản tấn công mạng và giải pháp DNSSEC với các kịch bản tấn công DNS đó.