

Case Studies จากผู้ให้บริการ Public DNS

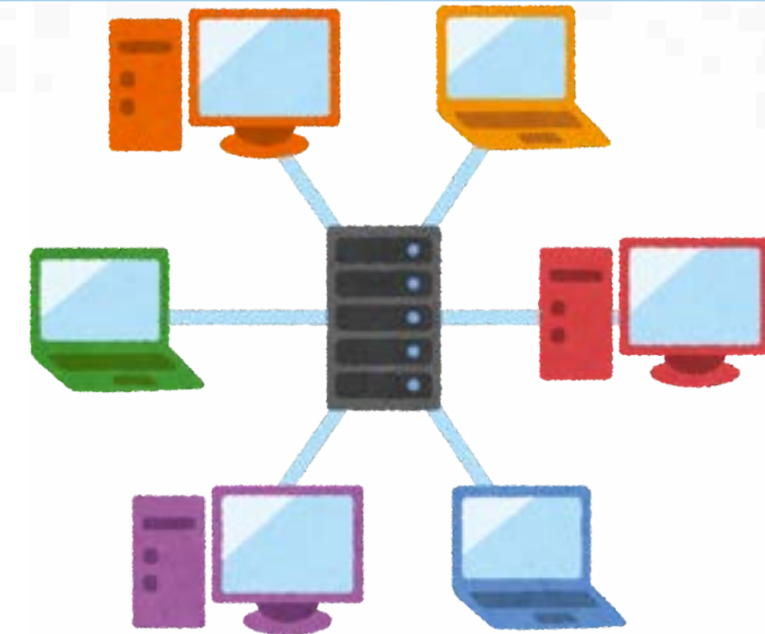
ฐิติพงศ์ ภาคอินทรีย์
ผู้จัดการฝ่ายสนับสนุนปฏิบัติการ
บริษัท ไทย เนม เซิร์ฟเวอร์ จำกัด



Thai Name Server Co.,Ltd.

ThaiNS Public DNS

- DNS Anycast
- EDNS Support
- IPv6 Support
- Domestic network
- DNSSEC Validation



double7.thains.co.th

203.159.77.77

2405:3340:e000::77:77



Thai Name Server Co.,Ltd.

ThaiNS Monitoring

- Network Monitoring
- Service Monitoring (DNS, DNSSEC)
- DNSSEC RRSIG



Thai Name Server Co.,Ltd.

ThaiNS Monitoring

- PING OK - Packet loss = 0%, RTA = 0.32 ms
- DNS Query time = 0 ms
- SOA OK = 0 [a.thains.co.th.:1241120048]-[expect:1241120048]
- No RRSIGs expiring in the next 2.5 days: (0.87s)



Thai Name Server Co.,Ltd.



กรณีศึกษา DNSSEC กับ Email



Thai Name Server Co.,Ltd.



กรณีศึกษา DNSSEC กับ Email (1)

NOC

- พบปัญหา Network
 - ค่า PING Latency สูงขึ้น หรือ PING LOSS เป็นช่วงสั้นๆ หรือ ค่า PING ปกติ
- พบปัญหา DNS Query
 - พบปัญหา communications error จาก network บางส่วน

```
$ dig @122.155.23.64 th soa +dnssec
;; communications error to 122.155.23.64#53: timed out
;; communications error to 122.155.23.64#53: timed out
;; communications error to 122.155.23.64#53: timed out
; <<> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<> @122.155.23.64 th soa +dnssec
; (1 server found)
;; global options: +cmd
;; no servers could be reached
```

กรณีศึกษา DNSSEC กับ Email (2)

NOC

- ตรวจสอบ PING / TRACE / MTR / DIG จาก Network ที่แตกต่างกัน
กัน ทั้งใน และต่างประเทศ

```
$ ping 122.155.23.64
PING (122.155.23.64) 56(84) bytes of data.
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=1 ttl=52 time=27.6 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=2 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=3 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=4 ttl=52 time=26.9 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=5 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=6 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=7 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=8 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=9 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=10 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=11 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=12 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=13 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=14 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=15 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=16 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=17 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=18 ttl=52 time=26.8 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=19 ttl=52 time=26.9 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=20 ttl=52 time=26.8 ms
```

SPG

```
$ ping 122.155.23.64
PING (122.155.23.64) 56(84) bytes of data.
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=1 ttl=45 time=312 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=2 ttl=45 time=304 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=3 ttl=45 time=308 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=4 ttl=45 time=308 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=5 ttl=45 time=308 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=6 ttl=45 time=322 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=8 ttl=45 time=320 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=9 ttl=45 time=317 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=10 ttl=45 time=299 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=11 ttl=45 time=298 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=12 ttl=45 time=310 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=13 ttl=45 time=311 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=14 ttl=45 time=322 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=15 ttl=45 time=309 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=16 ttl=45 time=304 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=17 ttl=45 time=321 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=18 ttl=45 time=307 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=19 ttl=45 time=317 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=20 ttl=45 time=322 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=21 ttl=45 time=305 ms
64 bytes from a.thains.co.th (122.155.23.64): icmp_seq=22 ttl=45 time=316 ms
```

NYC



Thai Name Server Co.,Ltd.

กรณีศึกษา DNSSEC กับ Email (3)

NOC

- ตรวจสอบ PING / TRACE / MTR / DIG จาก Network ที่แตกต่างกัน ทั้งใน และต่างประเทศ

```
$ mtr 122.155.23.64
ubuntu-s-lvcpu-1gb-sgp1-01 (157.245.202.104) -> 122.155.23.64 (122.155.23.62024-05-15T02:59:08+0000)
Keys: Help  Display mode  Restart statistics  Order of fields  quit
Packets
Host      Loss%  Snt  Last  Avg  Best  Wrst StDev
1. (waiting for reply)
2. 10.76.195.158      0.0%  100  0.5  0.7  0.3  12.3  1.2
3. 143.198.252.6      0.0%  100  0.4  0.4  0.3  0.8  0.1
4. 143.244.192.178    0.0%  100  0.3  0.4  0.3  4.8  0.5
5. 143.244.224.236    0.0%  100  1.0  0.9  0.7  2.3  0.2
6. 143.244.224.211    0.0%  100  0.6  0.6  0.5  5.5  0.5
7. 4651.sgw.equinix.com 0.0%  100  1.2  1.0  0.7  1.5  0.2
8. 61.19.9.133        0.0%  100  28.1 27.8 27.5 29.6 0.3
9. 122.155.225.66     0.0%  100  27.3 27.6 27.3 31.3 0.6
10. 122.155.30.122    0.0%  100  25.4 26.2 25.1 61.1 3.6
11. 122.155.23.44     0.0%  99  27.1 27.1 26.8 29.5 0.6
12. a.thains.co.th    0.0%  99  28.3 27.1 26.8 30.5 0.6
```

SPG

```
$ mtr 122.155.23.64
ubuntu-s-lvcpu-1gb-nyc3-01 (167.71.89.66) -> 122.155.23.64 2024-05-15T03:06:36+0000
Keys: Help  Display mode  Restart statistics  Order of fields  quit
Packets
Host      Loss%  Snt  Last  Avg  Best  Wrst StDev
1. (waiting for reply)
2. 10.74.132.63      0.0%  83  0.4  1.1  0.3  33.3  3.9
3. 138.197.248.254   30.1%  83  0.9  6.6  0.8  60.5  12.4
4. 143.244.192.172    0.0%  83  0.5  0.4  0.3  0.9  0.1
5. 143.244.225.216    0.0%  83  1.0  1.0  0.8  1.5  0.1
6. 143.244.225.143    0.0%  83  0.6  0.7  0.6  2.4  0.2
7. 10gigabitethernet1-2.core1.nyc6.he.net 80.5%  83  6.0  1.8  1.3  6.0  1.1
8. port-channel4.core2.nyc4.he.net 95.1%  83  5.2  4.6  1.3  10.5  4.3
9. port-channel11.core2.ash1.he.net 95.1%  83  6.2  7.1  6.2  8.7  1.1
10. port-channel17.core2.lax1.he.net 98.8%  83  61.4 61.4 61.4 61.4 0.0
11. 100ge0-71.core3.lax2.he.net 89.0%  83  78.1 70.8 67.2 78.1 4.0
12. 100ge0-62.core2.hkg1.he.net 98.8%  83  261.7 261.7 261.7 261.7 0.0
13. cat-telecom-public-company-ltd.10gig 46.3%  83  258.7 258.2 213.3 276.2 10.3
14. 61.19.9.121      6.1%  83  303.6 301.8 248.2 318.6 10.6
15. 122.155.225.54     9.8%  83  304.9 303.5 250.2 319.5 11.3
16. 122.155.30.134    11.0%  83  306.5 305.0 251.2 322.9 11.1
17. 122.155.23.44     7.3%  83  305.1 303.3 250.3 319.8 11.2
18. a.thains.co.th     9.8%  83  306.5 303.4 252.3 318.8 11.2
```

NYC

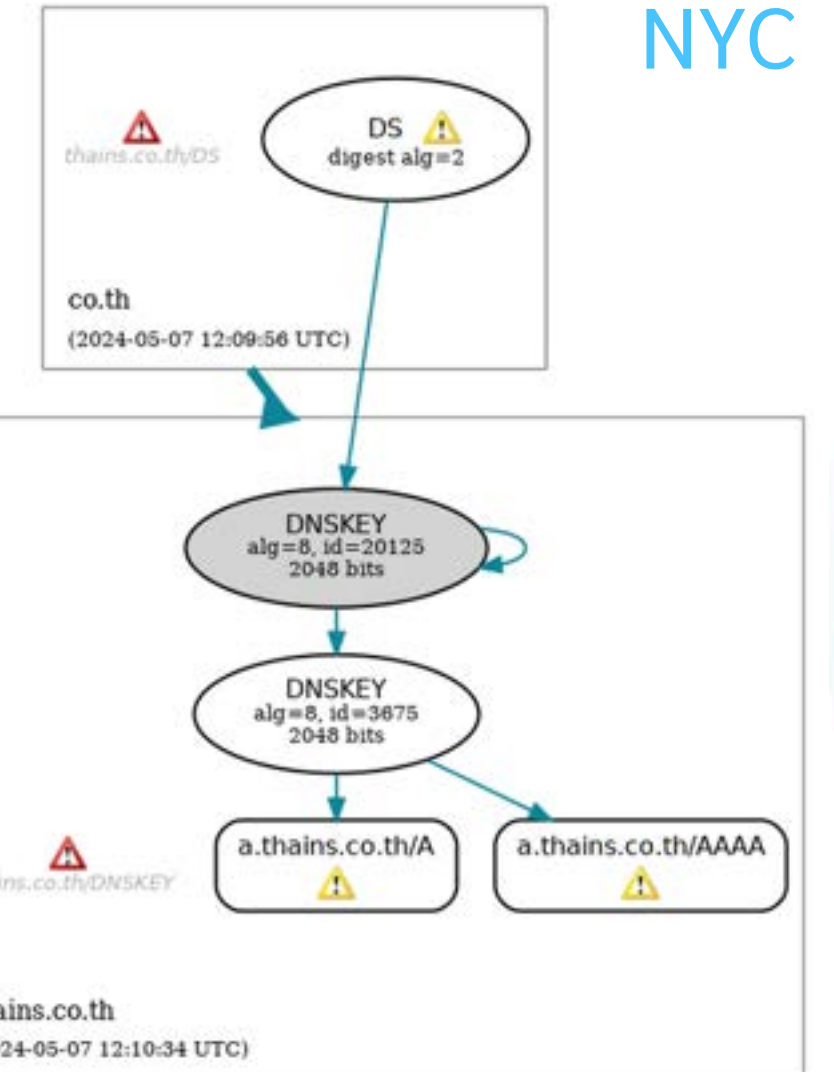
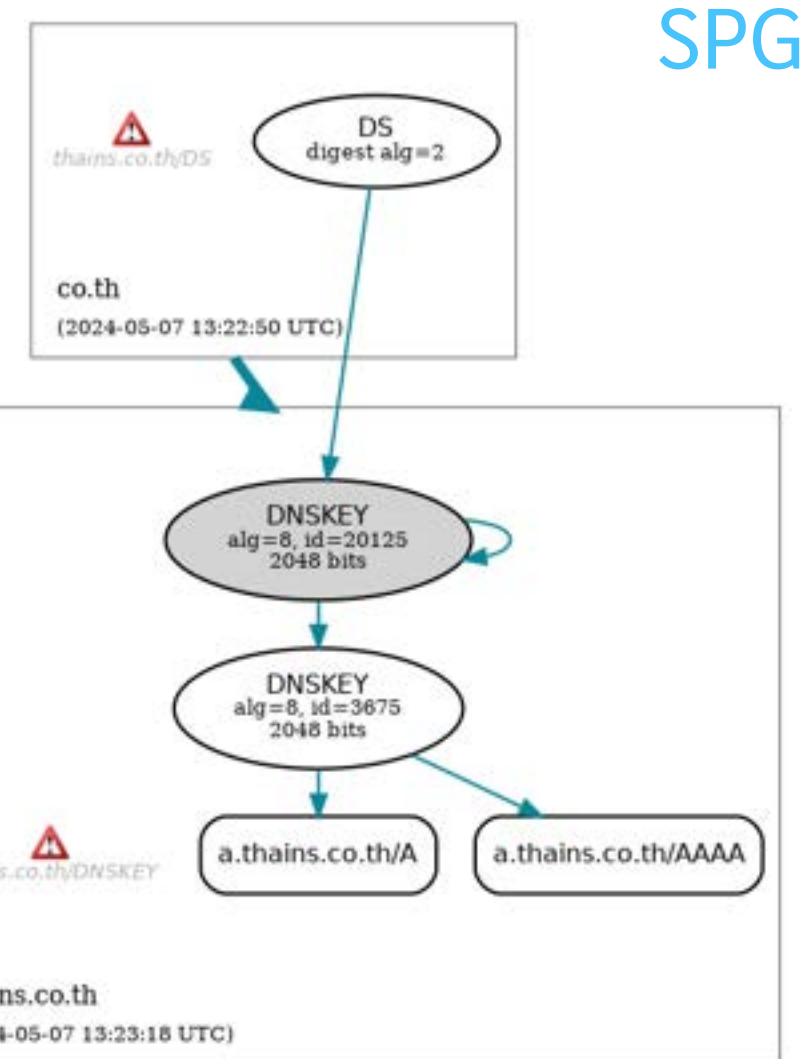
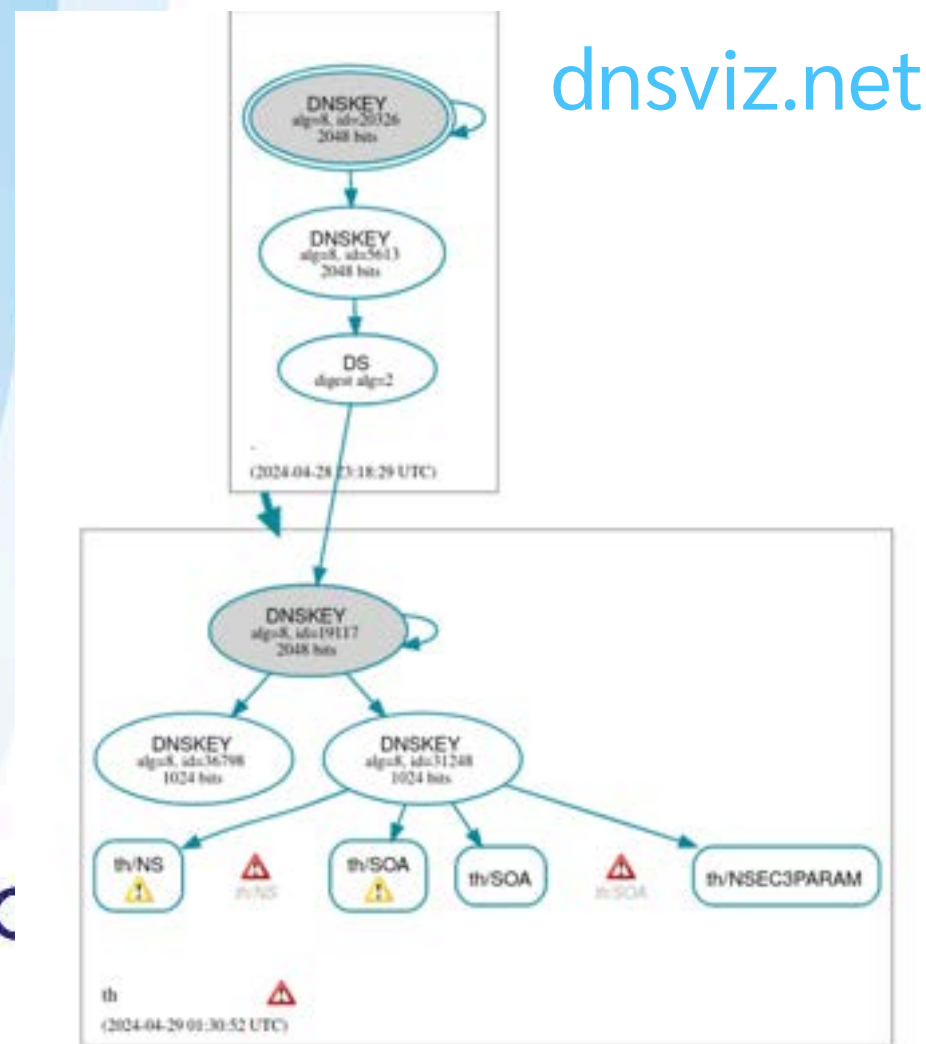


Thai Name Server Co.,Ltd.

กรณีศึกษา DNSSEC กับ Email (4)

NOC

- ตรวจสอบ DNSVIZ จาก Network ที่แตกต่างกัน



Thc

กรณีศึกษา DNSSEC กับ Email (5)

ISP / IIG

- ทาง ISP ทดสอบค่า PING จะปกติ
- ไม่พบการแจ้งเตือน Domestic Network ทำงานผิดปกติ
- Network ต่างประเทศเปลี่ยน Route
 - Network หลักมีปัญหา
 - Cable ใต้ทะเลขาด



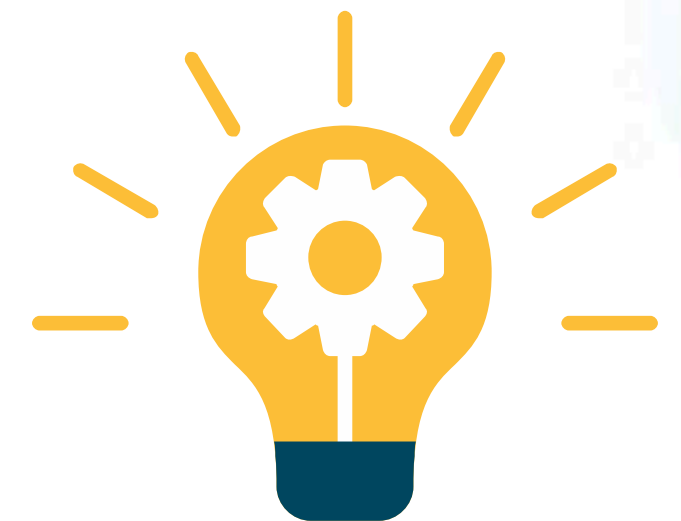
Thai Name Server Co.,Ltd.

กรณีศึกษา DNSSEC กับ Email (6)

- NOC ISP / IIG
 - ทดสอบ PING, TRACE จาก Router / Network Device
 - PING ใช้ ICMP
- NOC ThaiNS / System Admin / Engineer
 - ทดสอบ DNS Service จากบน Server
 - DNS ใช้ UDP
 - DNSSEC packet size ใหญ่กว่า DNS



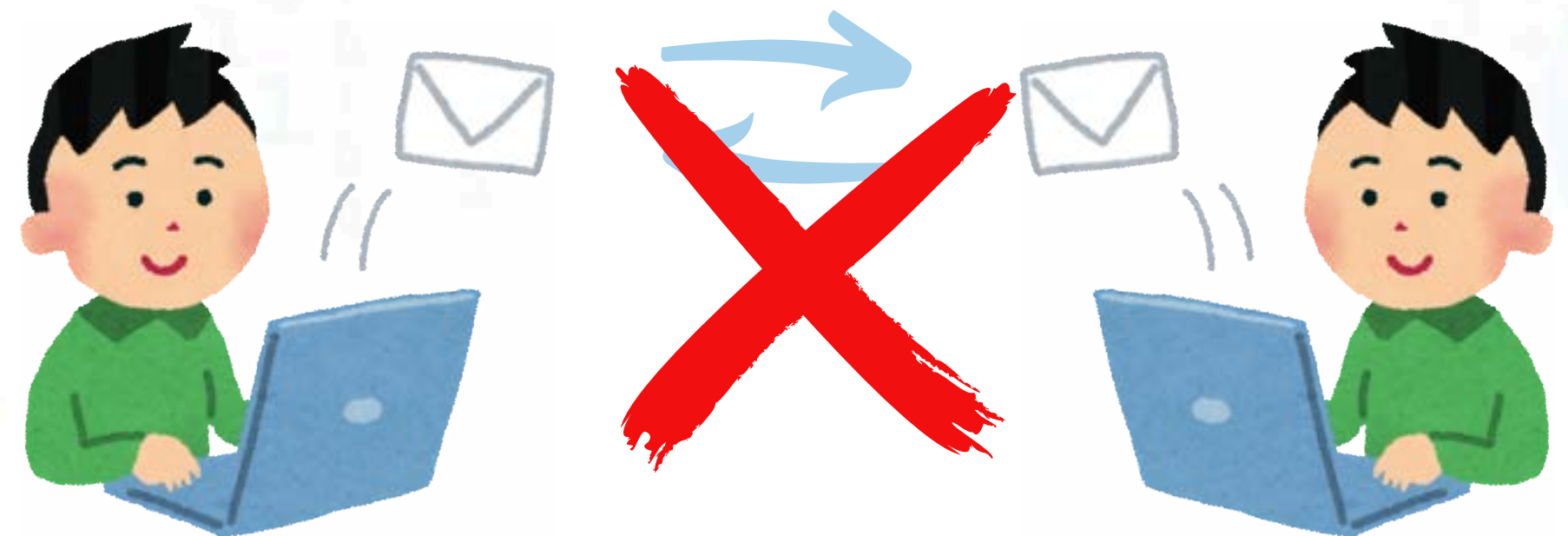
Thai Name Server Co.,Ltd.



กรณีศึกษา DNSSEC กับ Email (7)

ผู้ใช้งาน

- รับอีเมล ไม่ได้
- Email Server ไม่สามารถ Lookup Domain
- กว่าจะรู้ตัวว่าไม่ได้รับอีเมล



Thai Name Server Co.,Ltd.

กรณีศึกษา DNSSEC กับ Email (8)

IT Support / System Admin / System Engineer

- ตรวจสอบเครื่องผู้ใช้งาน ✓
- ตรวจสอบ Network ✓
- ตรวจสอบระบบอีเมล ✓
- ตรวจสอบระบบ DNS ✗



Thai Name Server Co.,Ltd.



กรณีศึกษา DNSSEC กับ Email (9)

การแก้ไขปัญหา

NOC <--> ISP

- พิสูจน์กับ ISP สาเหตุเกิดจาก Network เปลี่ยน Route ทำให้ DNSSEC Query ไม่ได้
- เพื่อให้ ISP เปลี่ยน Route ให้ DNSSEC Query ได้



Thai Name Server Co.,Ltd.

กรณีศึกษา DNSSEC กับ Email (10)

ทำไม DNSSEC ถึง Query ไม่ได้เมื่อ Route เปลี่ยน ?

- high network latency
- network ไม่ stable
- อุปกรณ์ Network ไม่รองรับ



กรณีศึกษา DNSSEC กับ Email (11)

การแก้ไขปัญหา

User <---> IT Support / System Admin / System Engineer

- แก้ไขเครื่องของ User ใช้งานได้
- เปลี่ยน Network
- เปลี่ยน DNS



Thai Name Server Co.,Ltd.

กรณีศึกษา DNSSEC กับ Email (12)

สรุป

- ไม่มีใครคาดว่า การเปลี่ยน Route ของ Network จะส่งผลกระทบต่อ DNSSEC Service ทำให้การแก้ไขปัญหาค้างนาน
- ถ้าระบบส่วนใหญ่ใช้งาน DNSSEC จะทำให้ตรวจสอบสาเหตุของปัญหาได้เร็วขึ้น เพราะจะเห็นผลกระทบได้ชัดเจน



Thai Name Server Co.,Ltd.

การตรวจสอบ DNSSEC

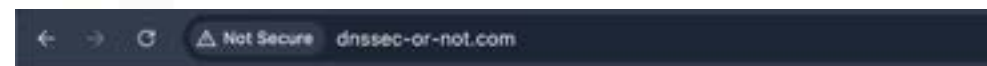


Thai Name Server Co.,Ltd.



ตรวจสอบ DNSSEC (1)

- <http://www.dnssec-or-not.com/>



Are you protected by DNSSEC? Or Not?

This page tests whether or not the DNS queries from your computer are protected with DNSSEC validation.

Very Nice! The test indicates you are protected by DNSSEC!



Are you protected by DNSSEC? Or Not?

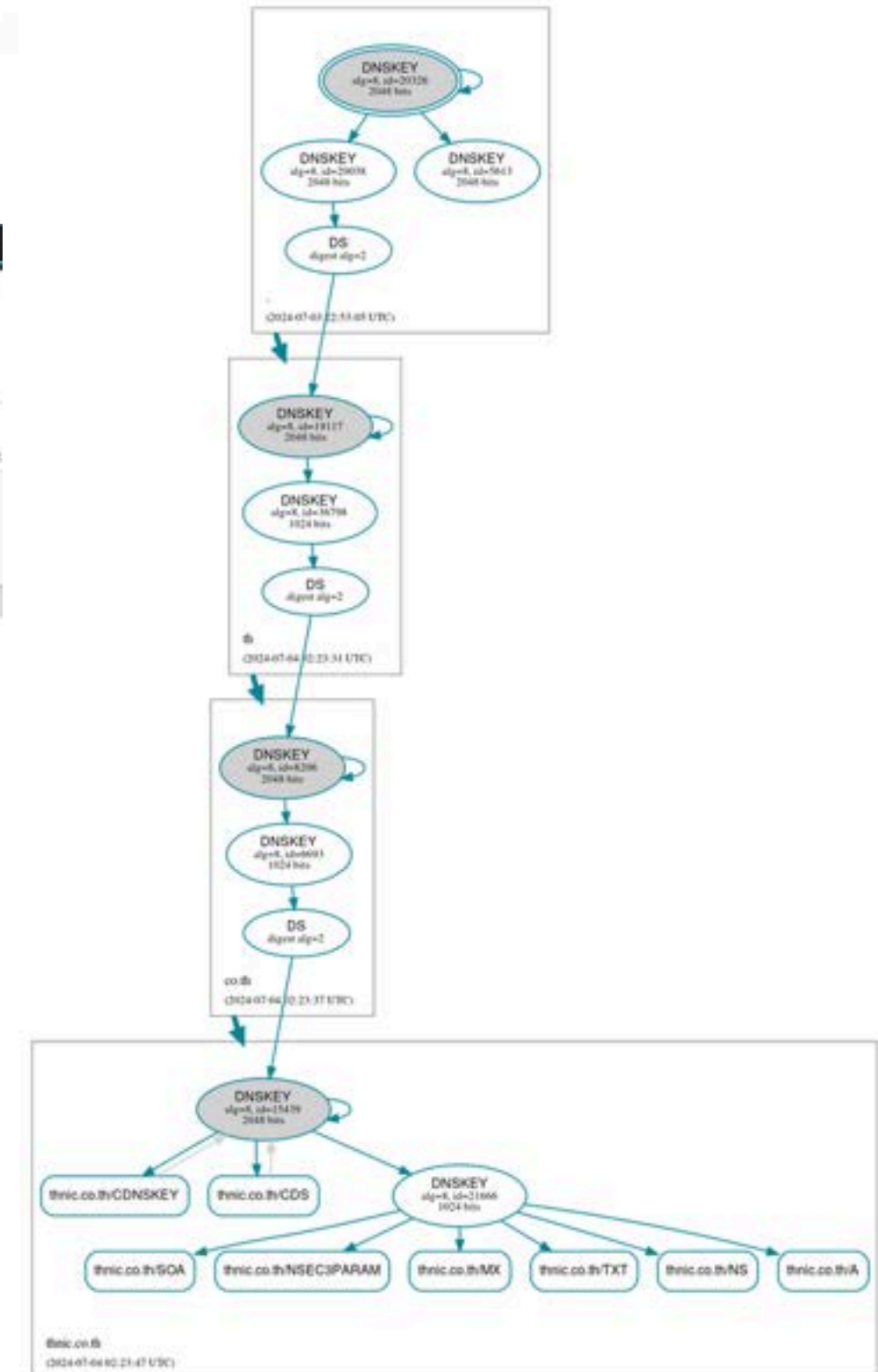
This page tests whether or not the DNS queries from your computer are protected with DNSSEC validation.

Sigh... the test indicates you are NOT protected.



ตรวจสอบ DNSSEC (2)

- <https://dnsviz.net/>



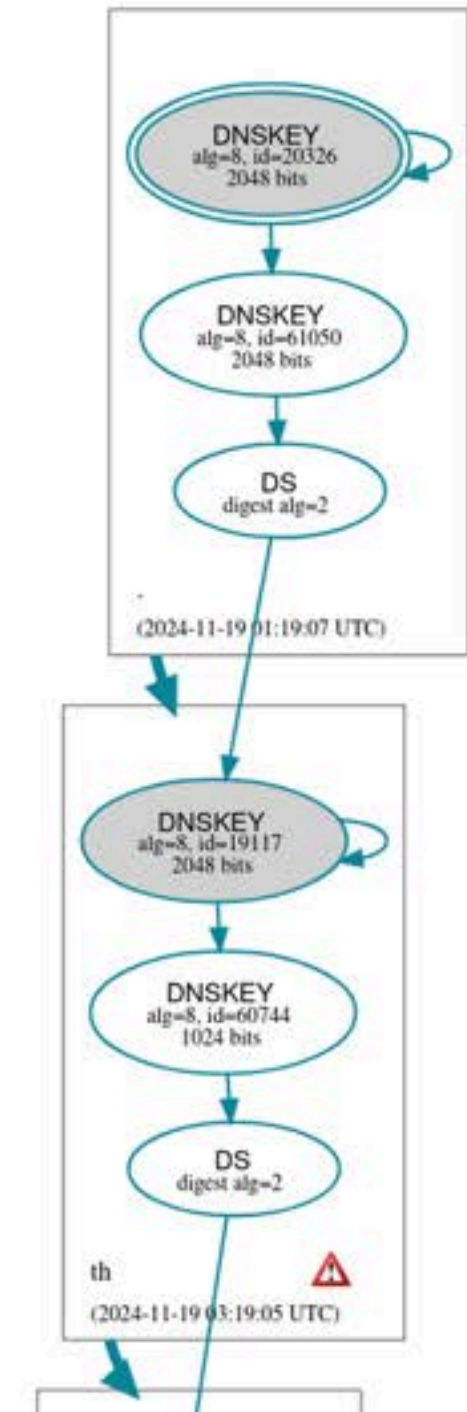
Thai Nar

ตรวจสอบ DNSSEC (3)

- <https://dnsviz.net/>

We found error : th zone: The server(s) were not responsive to queries over UDP. See RFC 1035, Sec. 4.2.

(2001:678:4::1c)



Thai Name Server Co.,Ltd.

ตรวจสอบ DNSSEC (4)

- <https://dnssec-debugger.verisignlabs.com/>

Analyzing DNSSEC problems for **thains.co.th**

.	<ul style="list-style-type: none"> Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
th	<ul style="list-style-type: none"> Found 1 DS records for th in the . zone DS=19117/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=61050 and DNSKEY=61050 verifies the DS RRset Found 2 DNSKEY records for th DS=19117/SHA-256 verifies DNSKEY=19117/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19117 and DNSKEY=19117/SEP verifies the DNSKEY RRset
co.th	<ul style="list-style-type: none"> Found 1 DS records for co.th in the th zone DS=8206/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=60744 and DNSKEY=60744 verifies the DS RRset Found 2 DNSKEY records for co.th DS=8206/SHA-256 verifies DNSKEY=8206/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=8206 and DNSKEY=8206/SEP verifies the DNSKEY RRset
thains.co.th	<ul style="list-style-type: none"> Found 1 DS records for thains.co.th in the co.th zone DS=20125/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=4443 and DNSKEY=4443 verifies the DS RRset Found 2 DNSKEY records for thains.co.th DS=20125/SHA-256 verifies DNSKEY=20125/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20125 and DNSKEY=20125/SEP verifies the DNSKEY RRset ns2.thains.co.th is authoritative for thains.co.th thains.co.th A RR has value 203.159.64.46 Found 1 RRSIGs over A RRset RRSIG=53328 and DNSKEY=53328 verifies the A RRset
thains.co.th	<ul style="list-style-type: none"> ns1.thains.co.th is authoritative for thains.co.th thains.co.th A RR has value 203.159.64.46 Found 1 RRSIGs over A RRset RRSIG=53328 and DNSKEY=53328 verifies the A RRset



Thai Name Server Co.,Ltd.

ตรวจสอบ DNSSEC (5)

DNSSEC Key Monitor

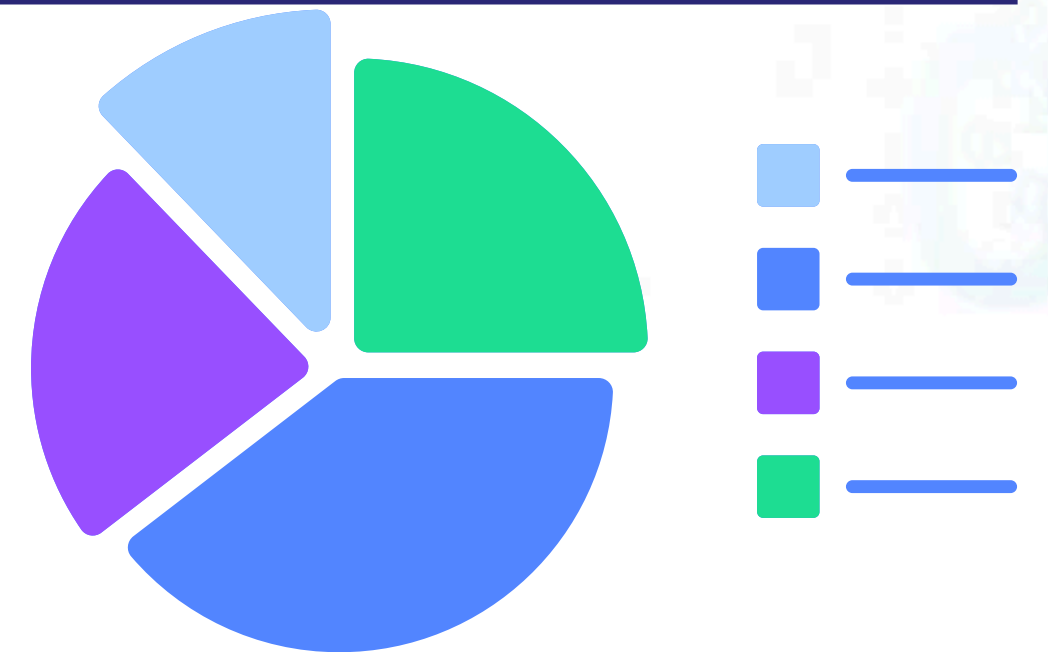
- <https://github.com/DNS-OARC/tldmon>

Host	Service	Status	Last Check	Duration	Attempt	Status Information
th	AA	OK	11-19-2024 07:13:52	487d 23h 34m 26s	1/3	6 nameservers are authoritative: (2.78s)
	EDNS	OK	11-19-2024 07:20:57	161d 18h 40m 51s	1/3	6 nameservers support EDNS0: (9.26s)
	LAME	OK	11-19-2024 07:24:32	487d 23h 28m 58s	1/3	6 nameservers are not lame: (1.16s)
	NSSET	OK	11-19-2024 07:26:36	487d 23h 26m 15s	1/3	6 nameservers have consistent NS RRset: (3.56s)
	OPENRES	OK	11-19-2024 07:27:06	487d 23h 23m 31s	1/3	6 nameservers are closed to recursion: (44.72s)
	QTYPE	OK	11-19-2024 07:29:09	0d 2h 28m 8s	1/3	b.thains.co.th reports OK
	RCODE	OK	11-19-2024 07:10:06	2d 1h 47m 12s	1/3	6 nameservers responding: (1.15s)
	RRSIG	OK	11-19-2024 07:29:55	2d 1h 27m 22s	1/3	No RRSIGs expiring in the next 2.5 days: (1.28s)
	SERIAL	OK	11-19-2024 07:55:08	2d 2h 2m 10s	1/3	6 nameservers have serial 1241119030: (5.02s)
	TCP	OK	11-19-2024 06:59:43	9d 23h 57m 35s	1/3	6 nameservers support TCP: (3.07s)
	Wildcard	OK	11-19-2024 05:01:15	487d 23h 37m 9s	1/3	OK: *.th returns NXDOMAIN (0.2 sec)



Thai Name Server Co.,Ltd.

สถิติ DNSSEC จาก ThaiNS Public DNS

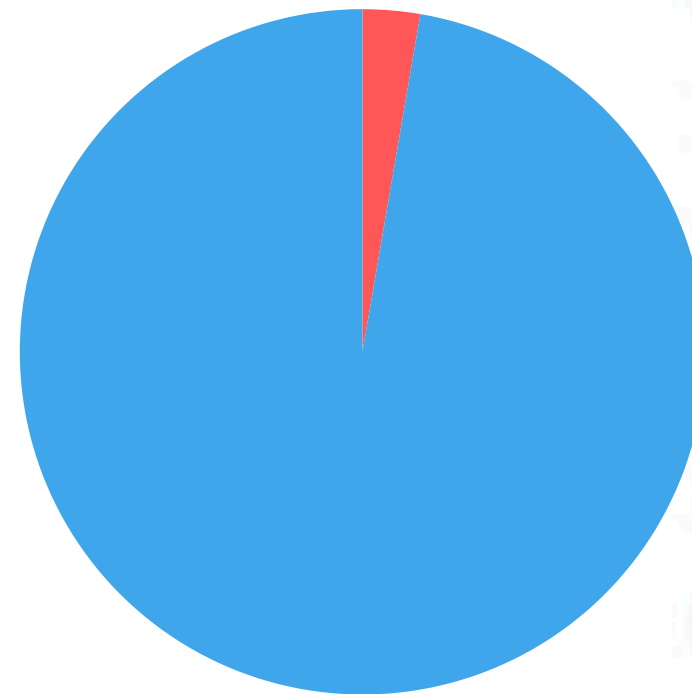


Thai Name Server Co.,Ltd.

สถิติ DNSSEC (1)

Aug 2024

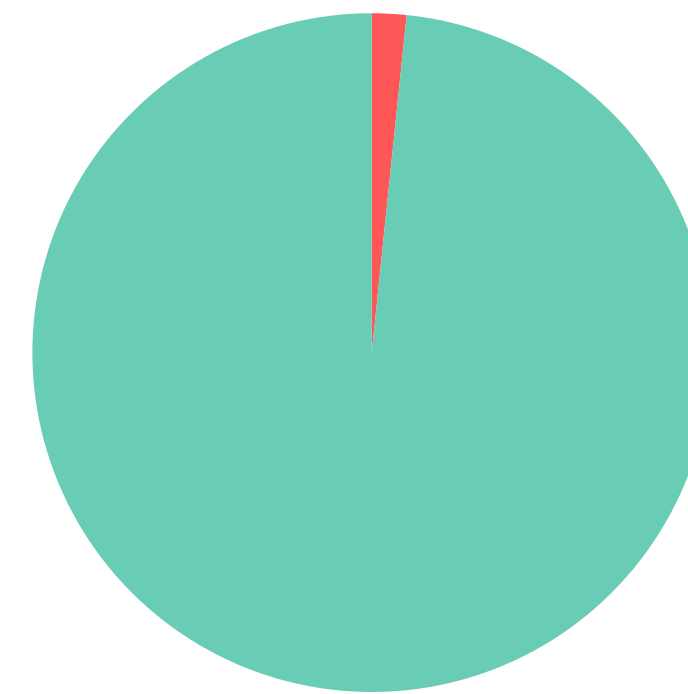
DNSSEC Validation
2.7%



DNS
97.3%

Nov 2024

DNSSEC Validation
1.6%



DNS
98.4%

Thai Name Server Co.,Ltd.

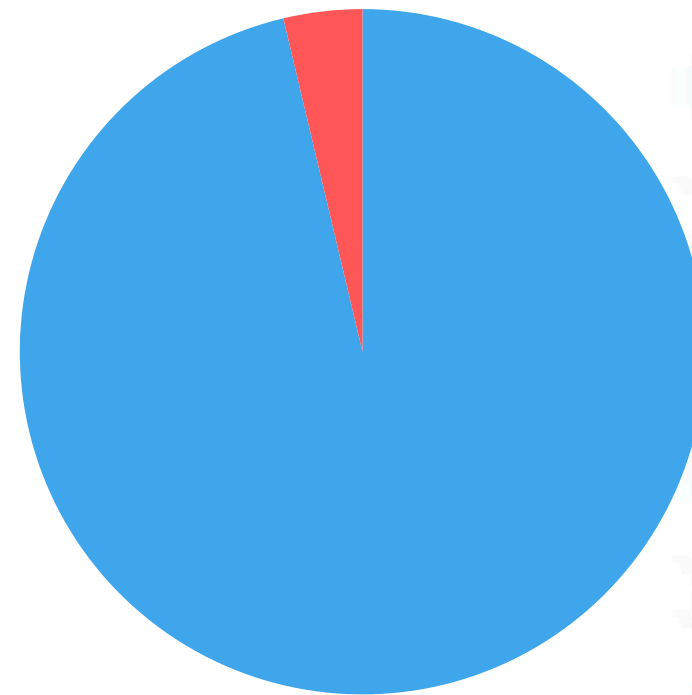
ข้อมูลจาก ThaiNS Public DNS



สถิติ DNSSEC (2)

Aug 2024

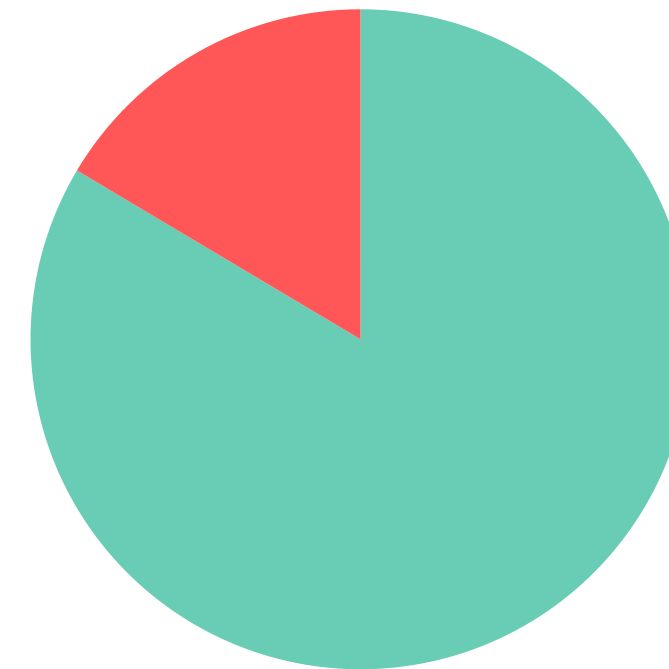
DNSSEC Validation Fail
3.7%



DNSSEC Validation Success
96.3%

Nov 2024

DNSSEC Validation Fail
16.5%



DNSSEC Validation Success
83.5%

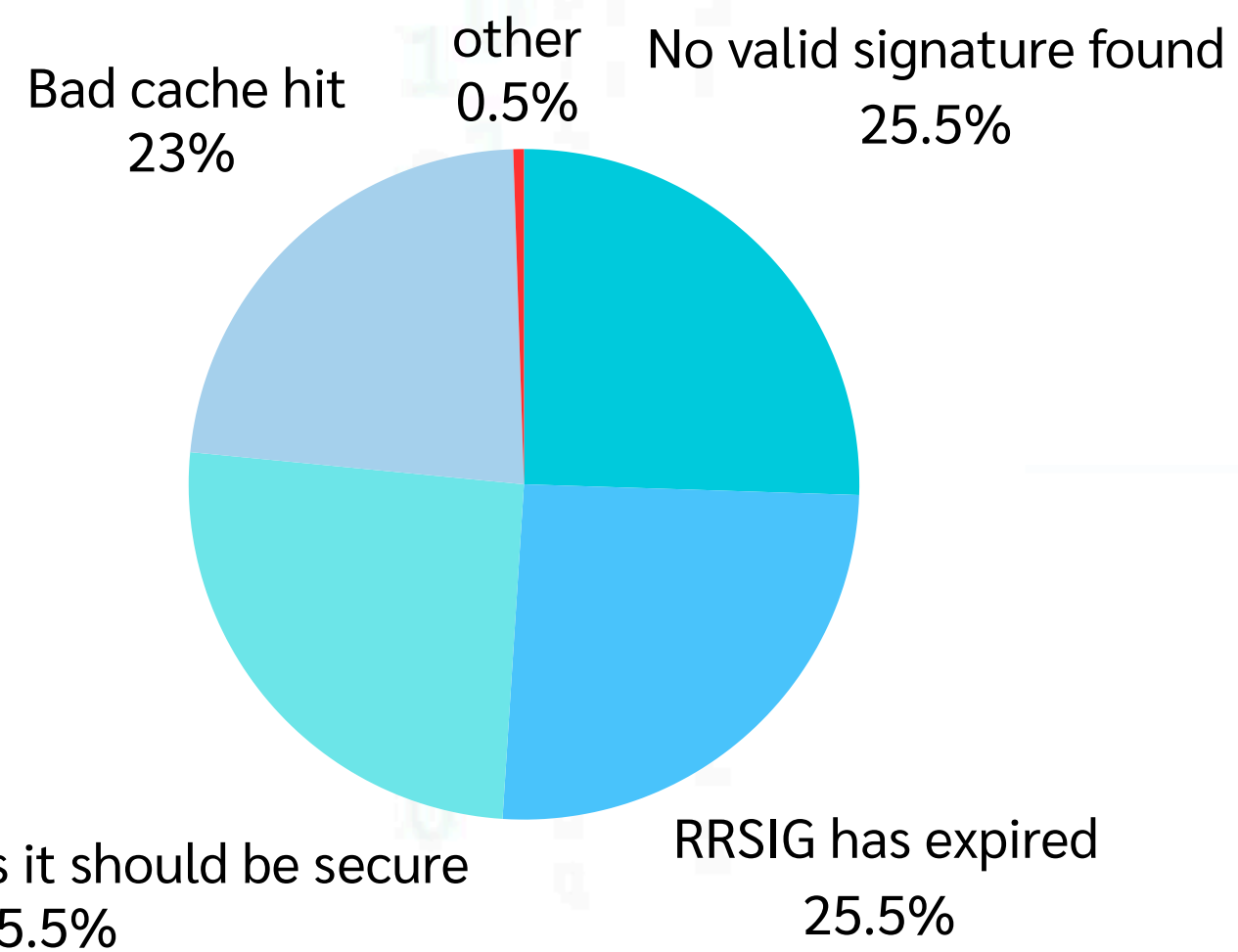


Thai Name Server Co.,Ltd.

ข้อมูลจาก ThaiNS Public DNS

สถิติ DNSSEC (3)

Aug 2024



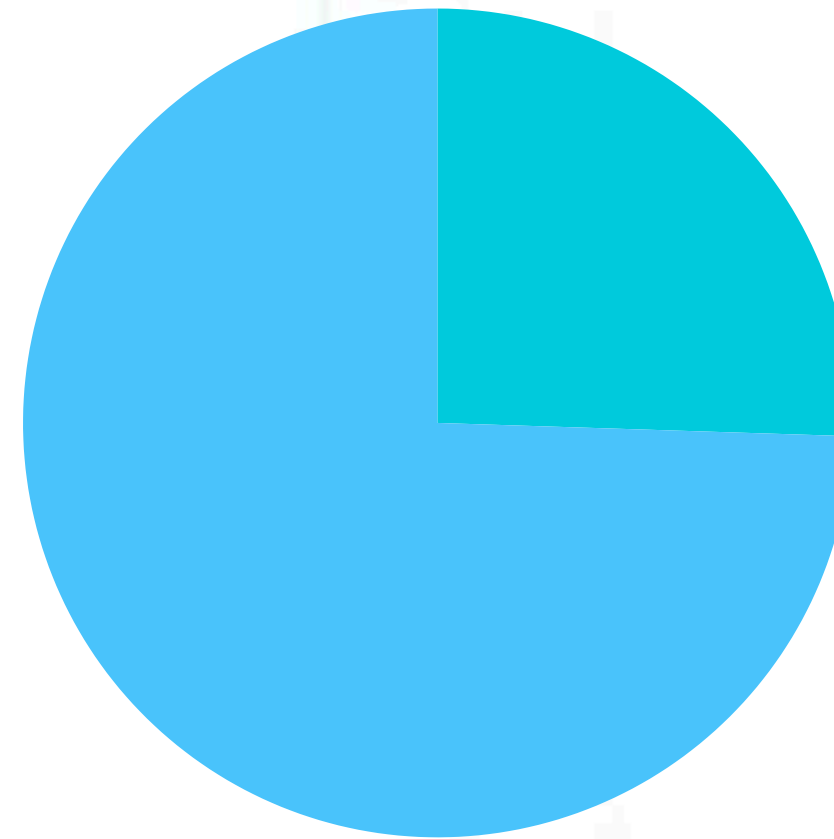
Thai Name Server Co.,Ltd.

ข้อมูลจาก ThaiNS Public DNS

สถิติ DNSSEC (4)

Aug 2024

.th DNSSEC validation Fail
25.5%



other DNSSEC validation Fail
74.5%

Thai Name Server Co.,Ltd.

ข้อมูลจาก ThaiNS Public DNS



แนวทางแก้ปัญหา

- แนวทางการตั้งค่า dnssec validation ฝั่ง client Site ให้รองรับการใช้งาน
- กรณี dnssec ฝั่ง Server Site มีปัญหา เช่น dnskey expired



Thai Name Server Co.,Ltd.

แนวทางแก้ปัญหา

BLUECAT

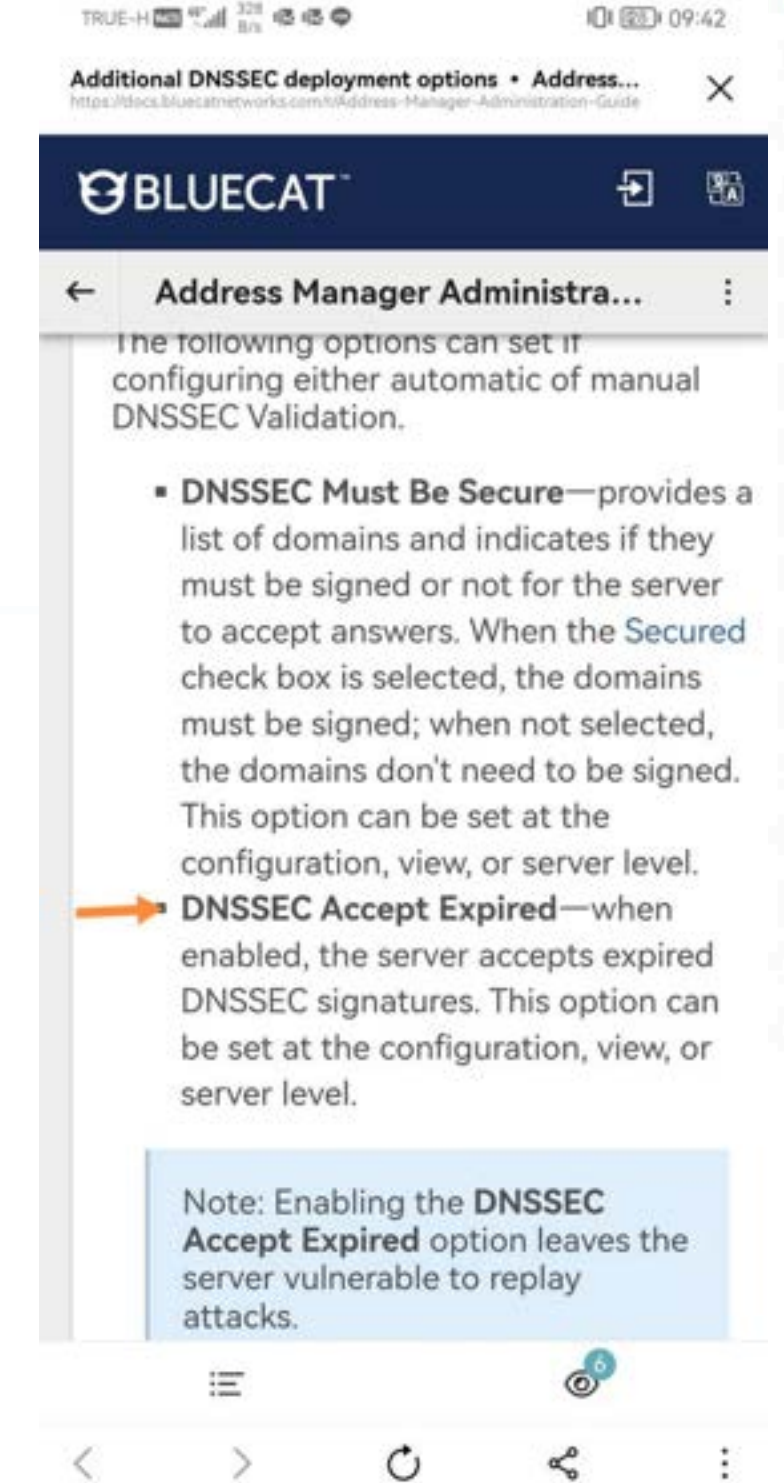
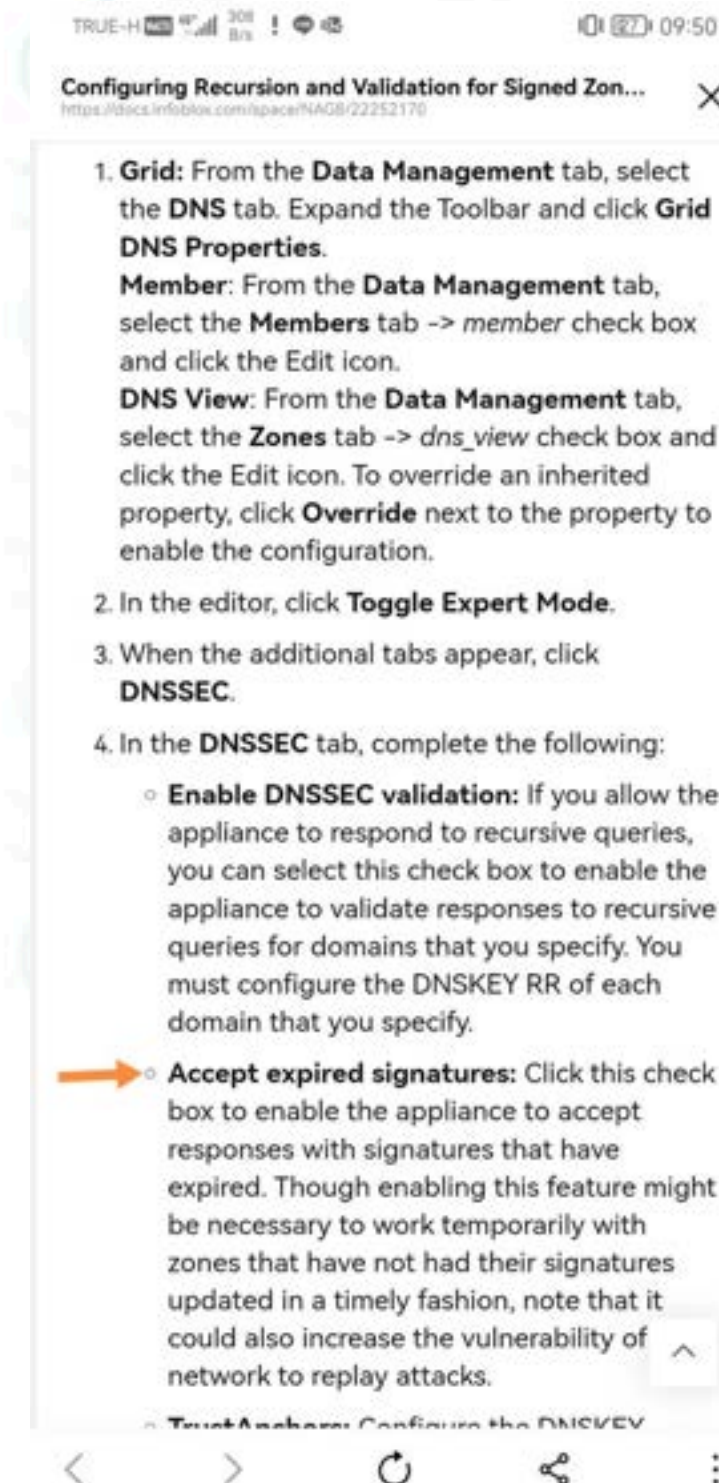
- bluecatnetworks.com

Infoblox

- infoblox.com



Thai Name Server Co.,Ltd.



แนวทางแก้ปัญหา

Bind

- <https://www.isc.org/bind/>

```
options {  
    ...  
    dnssec-validation auto;  
    ...  
};
```



Thai Name Server Co.,Ltd.

ตัวอย่าง Log Validation

```
validating t[REDACTED]cz/A: no valid signature found
validating [REDACTED]/SOA: no valid signature found
validating [REDACTED]/NSEC: no valid signature found
validating biserici.live/SOA: no valid signature found
validating biserici.live/NSEC: no valid signature found
validating betesdachurchcom.biserici.live/NSEC: no valid signature found
```



```
validating [REDACTED]/DS: starting
validating [REDACTED]/DS: attempting negative response validation from message
validating CK0P0JMG874LJREF7EFN8430QVIT8BSM.com/NSEC3: starting
validating CK0P0JMG874LJREF7EFN8430QVIT8BSM.com/NSEC3: attempting positive response validation
validating CK0P0JMG874LJREF7EFN8430QVIT8BSM.com/NSEC3: keyset with trust secure
validating CK0P0JMG874LJREF7EFN8430QVIT8BSM.com/NSEC3: verify rdataset (keyid=59354): success
validating CK0P0JMG874LJREF7EFN8430QVIT8BSM.com/NSEC3: marking as secure, noqname proof not needed
validating [REDACTED]/DS: in validator_callback_nsec
validating [REDACTED]/DS: resuming validate_nx
validating com/SOA: starting
validating com/SOA: attempting positive response validation
validating com/SOA: keyset with trust secure
validating com/SOA: verify rdataset (keyid=59354): success
validating com/SOA: marking as secure, noqname proof not needed
validating [REDACTED]/DS: in validator_callback_nsec
validating [REDACTED]/DS: resuming validate_nx
validating AINBC9UMVNLLDANJFV782UNUBC9P86TM.com/NSEC3: starting
validating AINBC9UMVNLLDANJFV782UNUBC9P86TM.com/NSEC3: attempting positive response validation
validating AINBC9UMVNLLDANJFV782UNUBC9P86TM.com/NSEC3: keyset with trust secure
validating AINBC9UMVNLLDANJFV782UNUBC9P86TM.com/NSEC3: verify rdataset (keyid=59354): success
validating AINBC9UMVNLLDANJFV782UNUBC9P86TM.com/NSEC3: marking as secure, noqname proof not needed
```



Reference

DNSSEC Tools

- <https://www.internetsociety.org/deploy360/dnssec/tools/>

DNSSEC Debugger

- <https://dnssec-debugger.verisignlabs.com/>

DNSVIZ

- <https://dnsviz.net/>
- <https://github.com/dnsviz/dnsviz>

Thai Name Server Co.,Ltd.



Reference

DNSSEC-TRIGGER

- <https://www.nlnetlabs.nl/projects/dnssec-trigger/about/>



Thai Name Server Co.,Ltd.

ฐิติพงษ์ ภาคอินทรีย์
ผู้จัดการฝ่ายสนับสนุนปฏิบัติการ
บริษัท ไทย เนม เซิร์ฟเวอร์ จำกัด

Thank You

titipong@thains.co.th
noc@thains.co.th



Thai Name Server Co.,Ltd.