ANE voor e-mail security applicatie

Inhoud

Inleiding

Dit document beschrijft DANE-implementatie voor ESR-uitgaande poststroom.

Voorwaarden

Algemene kennis van de ESA-concepten en -configuratie.

Eisen voor de uitvoering van DANE:

- DNSSEC-compatibele DNS-oplossing
- ESA met Async OS 12.0 of nieuwer

Achtergrondinformatie

In het ESR 12 is DANE ingevoerd voor uitgaande postvalidatie.

DNS-gebaseerde verificatie van benoemde entiteiten (DANE).

- DANE is een protocol voor internetbeveiliging waarmee X.509 digitale certificaten kunnen worden aangesloten op domeinnamen met DNSSEC (RFC 6698)
- DNSSEC is een verzameling IETF-specificaties voor het beveiligen van DNS-records door het gebruik van cryptografie met openbare sleutel. (Zeer elementaire verklaring. RFC 4033, RFC 4034 en RFC 4035)

OVERWEGINGEN VOOR DE UITVOERING

Controleer of het ESA een dnssec-compatibele DNS-oplossing gebruikt.

DNS-mogelijkheid om dnssec/DANE-vragen uit te voeren is vereist om DANE te implementeren.

Om de DNS-EDANE-functie van het ESA te testen, kan een eenvoudige test worden uitgevoerd vanaf de aanmelding met ESA CLI.

De CLI-opdracht 'daneverify' voert de complexe vragen uit om te verifiëren of een domein in staat is om DANE-verificatie door te geven.

Deze opdracht kan met een bekend goed domein worden gebruikt om te bevestigen dat het ESA in staat is dnssec-vragen op te lossen.

ietf.org is een wereldwijd bekende bron . Door de opdracht 'daneverify' uit te voeren, wordt geverifieerd of de DNS-oplossing al dan niet mogelijk is.

GELDIGE PASS: RESULTATEN "DANE SUCCESS" VAN DANE-INGANGEN VOOR DNS-SERVER VOOR SETF.org

```
> daneverify ietf.org

SECURE MX record(mail.ietf.org) found for ietf.org
SECURE A record (4.31.198.44) found for MX(mail.ietf.org) in ietf.org
Connecting to 4.31.198.44 on port 25.
Connected to 4.31.198.44 from interface 216.71.133.161.
SECURE TLSA record found for MX(mail.ietf.org) in ietf.org
Checking TLS connection.
TLS connection established: protocol TLSv1.2, cipher ECDHE-RSA-AES256-GCM-SHA384.
Certificate verification successful
TLS connection succeeded ietf.org.
DANE SUCCESS for ietf.org
DANE verification completed.
```

ONGELDIG FAIL: RESULTATEN VAN "BOGUS"-SERVER, NIET-DANE OPGENOMEN DNS-SERVER VOOR SETF.org

```
> daneverify ietf.org

BOGUS MX record found for ietf.org
DANE FAILED for ietf.org
DANE verification completed.
```

GELDIG FAIL: daneverify cisco.com > cisco heeft geen DANE geïmplementeerd. Dit is het verwachte resultaat van een dnssec-compatibele resolutie.

```
> daneverify cisco.com

INSECURE MX record(alln-mx-01.cisco.com) found for cisco.com
INSECURE MX record(alln-mx-01.cisco.com) found. The command will still proceed.
INSECURE A record (173.37.147.230) found for MX(alln-mx-01.cisco.com) in cisco.com
Trying next MX record in cisco.com
INSECURE MX record(rcdn-mx-01.cisco.com) found for cisco.com
INSECURE MX record(rcdn-mx-01.cisco.com) found. The command will still proceed.
```

```
INSECURE A record (72.163.7.166) found for MX(rcdn-mx-01.cisco.com) in cisco.com
Trying next MX record in cisco.com
INSECURE MX record(aer-mx-01.cisco.com) found for cisco.com
INSECURE MX record(aer-mx-01.cisco.com) found. The command will still proceed.
INSECURE A record (173.38.212.150) found for MX(aer-mx-01.cisco.com) in cisco.com
DANE FAILED for cisco.com
DANE verification completed.
```

Als de bovenstaande testen "GELDIG" werken:

- Een voorzichtige benadering zou zijn om elk domein te testen voordat er een profiel voor het domein wordt toegevoegd.
- Een agressievere benadering zou zijn om DANE te configureren op het profiel met standaard doelcontrole en te zien wie er doorgeeft/faalt.

Mail Direction bepaalt of DSAN zal verifiëren.

Het beleid voor verzendende groep/Mail Flow met de "RELAY"-actie voert een DANE-verificatie uit.

Het beleid voor verzendende groep/Mail Flow dat de "ACCEPT"-actie heeft ingesteld, zal geen DANE-verificatie uitvoeren.

> **Voorzichtig:** Als de ESA de Desination Control "DANE" ingeschakeld heeft op het **Default Policy**, **bestaat er een risico van mislukte levering.** Als een intern eigendom gebied, zoals de in de RAT genoemde, door zowel RELAY als ACCEPT mail flow-beleid gaat, gecombineerd met de aanwezigheid van een MTP-route voor het domein.

MTP-routers

DANE zal vallen op MTP Routes tenzij de "Destination Host" in "USEDNS wordt gevormd."

DANE Opportunistisch zal de berichten niet verzenden, met daarin de Delivery Queue, totdat de uitbarstingtimer verloopt.

Waarom? DANE Verificatie wordt overgeslagen aangezien een MTP-route een wijziging van de echte bestemming is en DNS mogelijk niet correct kan gebruiken.

Oplossing: Bestemmingscontroleprofielen maken om expliciet DANE-verificatie uit te schakelen voor domeinen die MSTP-routers bevatten

DANE opportunistisch of DANE verplicht

De volgende raadplegingen worden uitgevoerd tijdens DANE-verificatie.

Elke verificatie levert inhoud om de volgende verificatie uit te voeren.

- MX Record lookup (OCR) controleert of > beveiligd, onveilig, Bogus
- Er wordt een record opgezocht indien >> Beveiligd onveilig > Bogus
- Het opgezocht TLSA-bestand verifieert of >> Beveiligd, onveilig, Bogus, NXDOMAIN
- Certificaat verifiëren > Succes, mislukt

Beveiliging:

- DNS heeft de aanwezigheid van een veilig record met een door RSIG gevalideerde RSIG DS en DNSKEY in de vertrouwensketen geverifieerd.

Onzeker:

- DNS bepaalt het domein dat geen dnssec enabled records heeft.

Bogus:

- Onvolledige, maar huidige dnssec-items kunnen niet worden geverifieerd.
- Ongeldige bestanden vanwege een verlopen toets.
- Ontbrekende gegevens of sleutel in de vertrouwensketen.

NXDOMAIN

- Geen record gevonden in DNS.

Een combinatie van de bovenstaande record-check en de verificatieresultaten bepalen "DANE Success | DANE Fail | DANE-terugslag naar TLS."

Bijvoorbeeld: Als er geen RSIG verzonden is, bijvoorbeeld de MX record van Mcom, wordt de parent zone (.com) gecontroleerd om te zien of Bijvoorbeeld.com een DNSKEY record heeft, wat erop wijst dat Bijvoorbeeld.com zijn records zou moeten ondertekenen. Deze validatie gaat door met de vertrouwensketen die eindigt met de essentiële verificatie van de basiszone (..).wordt bereikt, en de sleutels van de basiszone komen overeen met wat de ESA verwacht (harde gecodeerde waarden op de ESA, die automatisch worden bijgewerkt op basis van RFC5011).

DANE MANDATORY

MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed	DANE Fail
Secure	Secure	Insecure		DANE Fail
Secure	secure	NXDOMAIN		DANE Fail
Secure	Secure	Bogus		DANE Fail
Secure	Insecure			DANE Fail
secure	Bogus			DANE Fail
Insecure	Secure	Secure	Success	DANE Fail
Insecure	Secure	Secure	Fail	DANE Fail
Insecure	Secure	Insecure		DANE Fail
Insecure	Secure	NXDOMAIN		DANE Fail
Insecure	Secure	Bogus		DANE Fail
Insecure	Insecure			DANE Fail
Insecure	Bogus			DANE Fail
Bogus				DANE Fail

DANE MANDATORY

Opmerking: DANE OPPORTUNISTISCH **GEEFT NIET DE VOORKEUR**. Het gedeelte ACTIE van de onderstaande resultaten DANE FAIL levert geen verplicht of opportunistisch

resultaat op. De berichten blijven in de bezorgingswachtrij totdat de timer afloopt en de levering wordt beëindigd.

DANE OPPORTUNISTISCH

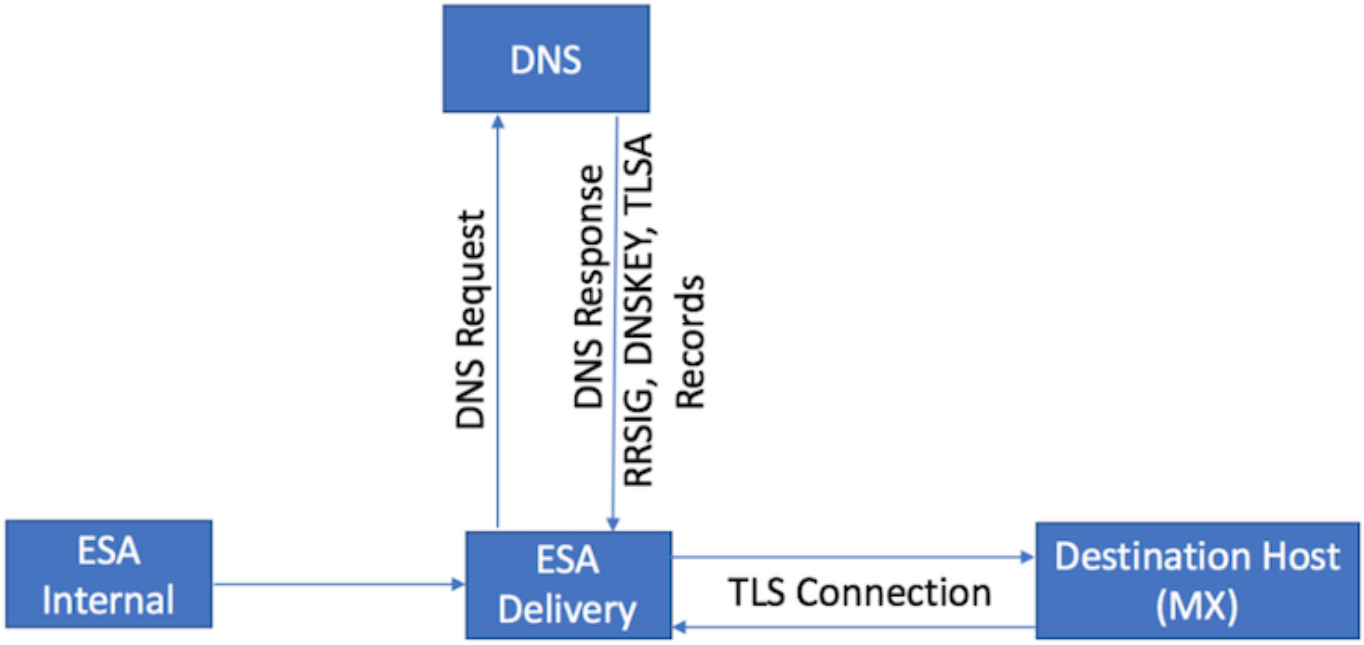
MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed →	DANE Fail
Secure	Secure	Insecure		Fallback to opportunistic TLS flow
Secure	secure	NXDOMAIN		Fallback to opportunisticTLS flow
Secure	Secure	Bogus	→	DANE Fail
Secure	Insecure	Mail will not be delivered for the marked arrows		Fallback to opportunistic TLS flow
secure	Bogus		→	DANE Fail
Insecure	Secure	Secure		Fallback to opportunisticTLS flow
Insecure	Secure	Insecure		Fallback to opportunisticTLS flow
Insecure	Secure	NXDOMAIN		Fallback to opportunisticTLS flow
Insecure	Secure	Bogus	→	DANE Fail
Insecure	Insecure			Fallback to opportunisticTLS flow
Insecure	Bogus			DANE Fail
Bogus			→	DANE Fail

DANE OPPORTUNISTISCH

DANE inschakelen bij meerdere applicatieomgevingen

Dit getal illustreert de werkstroom wanneer u DANE in een omgeving met meerdere apparaten in staat stelt.

Als de omgeving meerdere lagen ESA-apparatuur heeft, een voor scannen en een ander voor het leveren van berichten Zorg ervoor dat DANE alleen wordt geconfigureerd op het apparaat dat rechtstreeks verbonden is met de externe bestemmingen.



Multi-ESA ontwerp. DANE ingesteld op de Delivery ESA

Meervoudige DNS-oplossingen beheren

Als een ESA meerdere DNS-resoluties heeft geconfigureerd, een paar die DNSSEC ondersteunen welke DNSSEC niet ondersteunen, raadt Cisco aan om de DNSSEC-compatibele oplossers met een hogere prioriteit (lagere numerieke waarde) te configureren om inconsistenties te voorkomen.

Dit voorkomt dat de niet-DNSSEC geschikt is om het bestemmingsdomein dat DANE ondersteunt als 'Bogus' te classificeren.

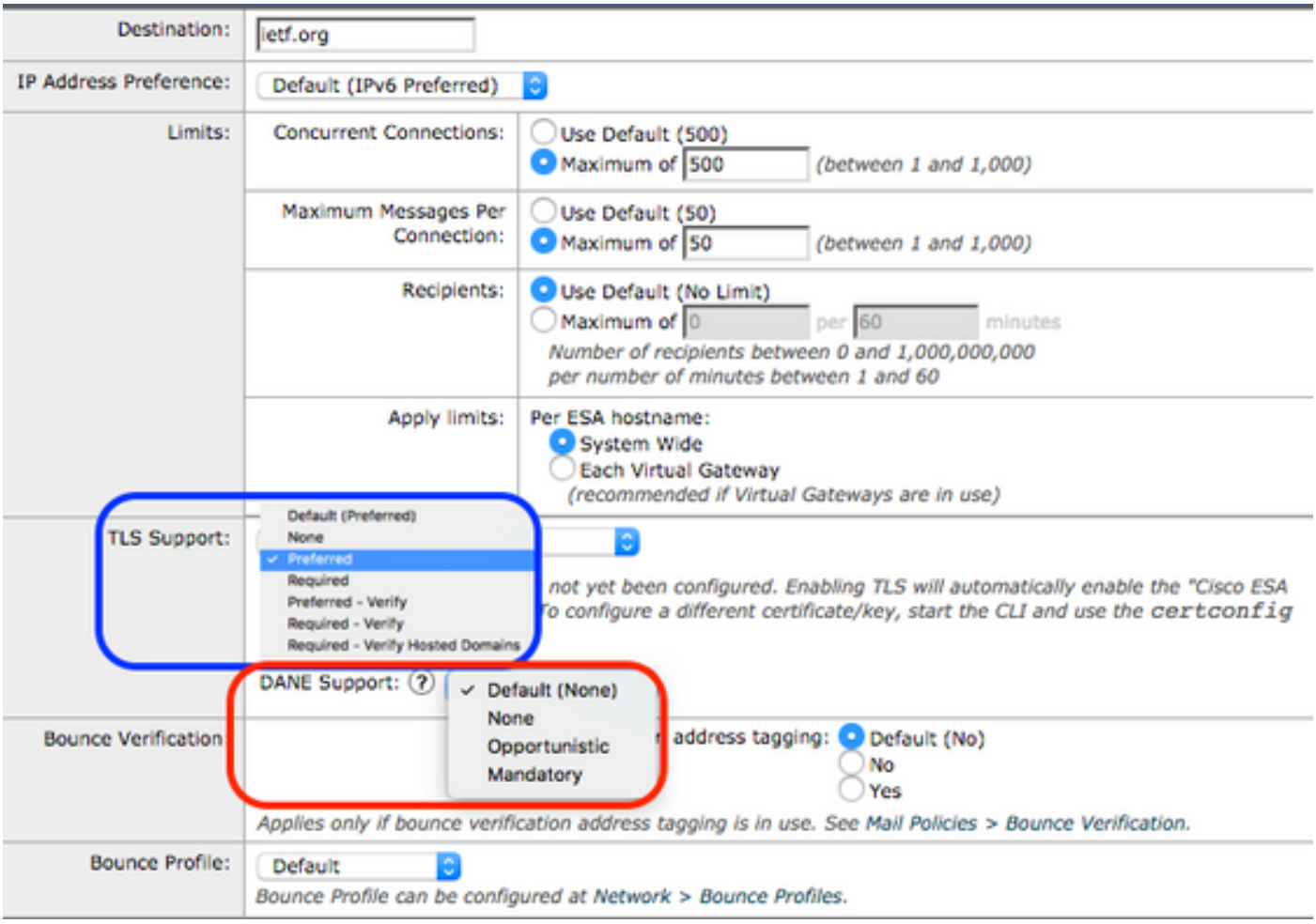
Secundaire DNS-server beheren

Wanneer de DNS-oplossing niet bereikbaar is, keert de DNS terug naar de secundaire DNS-server. Als u DNSSEC niet op de secundaire DNS server vormt, worden de MX records voor DANE-compatibele doeldomeinen geclassificeerd als ‘Bogus’. Dit beïnvloedt de levering van berichten ongeacht de DANE-instellingen (opportunistisch of verplicht). Cisco raadt u aan om een secundaire DNSSEC-kabelresolutie te gebruiken.

Configuratie

Configureer de ANE voor uitgaande poststroom.

1. Webei navigeren naar > Mail-beleid > Destination Control > Add Destination Destination
2. Vul het bovenste gedeelte van het profiel in naar uw voorkeur.
3. TLS-ondersteuning: **moet worden ingesteld op "TLS voorkeursbehandeling | Voorkeurig - Verificatie | Vereiste | Vereiste - Controleer| verplicht - controleer Hosted Domain**."
4. Nadat TLS-ondersteuning is ingeschakeld, ANE-ondersteuning: het uitrolmenu wordt actief.
5. **DANE-ondersteuning: opties omvatten "geen | opportunistisch | Verplicht.**
6. Nadat de optie ANE-ondersteuning is voltooid, kunt u wijzigingen indienen en doorgeven.



Bestemmingscontroleprofiel - DANE controleren

Controleer het DANE-succes

Leveringsstatus

Controleer het "Delivery Status" rapport van WebeiUI voor elke onbedoelde opbouw van doeldomeinen, mogelijk door DANE-falen.

Voer deze uit voordat u de service start, en onderbreek vervolgens enkele dagen lang de tijd om te garanderen dat de service nog altijd succesvol is.

ESA Webei > Monitor > Delivery Status > controleer de kolom "Actieve ontvangers".

Vastlegging e-mail

Standaard postlogbestanden op informatieniveau voor logniveau.

De maillogboeken tonen zeer subtiele indicatoren voor DANE die met succes in de onderhandelingen zijn gebracht.

De laatste uitloop van de TLS-onderhandeling zal een enigszins gewijzigde uitvoer omvatten om het domein aan het eind van de logingang op te nemen.

De logingang zal "TLS succesprotocol", gevolgd door TLS versie/algoritme "voor domain.com" bevatten.

De magie zit in de "voor":

```
myesa.local> grep "TLS success.*for" mail_logs

Tue Feb  5 13:20:03 2019 Info: DCID 2322371 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-
GCM-SHA384 for karakun.com
```

Vastlegging e.d.

Aangepaste Mail-Logs op Debug Level worden volledige raadpleging van DSAN en dnssec, onderhandeling verwacht, delen van de controle die worden doorgegeven/faalt en een succesindicator weergegeven.

> **Opmerking: Mail-logbestanden die zijn ingesteld voor Debug Level logging kunnen buitensporige bronnen in een ESA gebruiken afhankelijk van de systeembelasting en de configuratie.**

Mail-logbestanden die zijn ingesteld voor Debug Level logging kunnen buitensporige bronnen in een ESA gebruiken afhankelijk van de systeembelasting en de configuratie.

De e-mailbestanden worden doorgaans NIET langere tijd op Debug Level onderhouden.

De logbestanden op Debug Level kunnen in een korte tijd een enorm aantal postbestanden genereren.

Een frequente praktijk is om een extra logabonnement voor mail_logs_d te maken en de logbestand voor DEBUG in te stellen.

De actie voorkomt impact op de bestaande mail_logs en laat manipulatie op het volume van de blogs toe die voor het abonnement werden onderhouden.

Om het volume gemaakte logbestanden te controleren, beperkt u het aantal te onderhouden bestanden tot een kleiner aantal zoals 2-4 bestanden.

Wanneer de bewaking, proefperiode of probleemoplossing is voltooid, schakelt u het logbestand uit.

Mail-logbestanden ingesteld voor debug-niveau tonen zeer gedetailleerde DANE-uitvoer:

Success sample daneverify

```
daneverify ietf.org

SECURE MX record(mail.ietf.org) found for ietf.org
SECURE A record (4.31.198.44) found for MX(mail.ietf.org) in ietf.org
Connecting to 4.31.198.44 on port 25.
Connected to 4.31.198.44 from interface 194.191.40.74.
SECURE TLSA record found for MX(mail.ietf.org) in ietf.org
Checking TLS connection.
TLS connection established: protocol TLSv1.2, cipher DHE-RSA-AES256-GCM-SHA384.
Certificate verification successful
TLS connection succeeded ietf.org.
DANE SUCCESS for ietf.org
DANE verification completed.
```

debug level mail logs during the above 'daneverify' exeuction.
Sample output from the execution of the daneverify ietf.org will populate the dns lookups within the mail logs

```
Mon Feb 4 20:08:47 2019 Debug: DNS query: Q('ietf.org', 'MX')
Mon Feb 4 20:08:47 2019 Debug: DNS query: QN('ietf.org', 'MX', 'recursive_nameserver0.parent')
Mon Feb 4 20:08:47 2019 Debug: DNS query: QIP ('ietf.org','MX','194.191.40.84',60)
Mon Feb 4 20:08:47 2019 Debug: DNS query: Q ('ietf.org', 'MX', '194.191.40.84')
Mon Feb  4 20:08:48 2019 Debug: DNSSEC Response data([(0, 'mail.ietf.org.')], secure, 0, 1800)
Mon Feb 4 20:08:48 2019 Debug: DNS encache (ietf.org, MX, [(8496573380345476L, 0, 'SECURE', (0,
'mail.ietf.org'))])
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q('mail.ietf.org', 'A')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QN('mail.ietf.org', 'A',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QIP ('mail.ietf.org','A','194.191.40.84',60)
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q ('mail.ietf.org', 'A', '194.191.40.84')
Mon Feb  4 20:08:48 2019 Debug: DNSSEC Response data(['4.31.198.44'], secure, 0, 1800)
Mon Feb 4 20:08:48 2019 Debug: DNS encache (mail.ietf.org, A, [(8496573380345476L, 0, 'SECURE',
'4.31.198.44')])
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q('mail.ietf.org', 'AAAA')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QN('mail.ietf.org', 'AAAA',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QIP ('mail.ietf.org','AAAA','194.191.40.84',60)
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q ('mail.ietf.org', 'AAAA', '194.191.40.84')
Mon Feb 4 20:08:48 2019 Warning: Received an invalid DNSSEC Response:
DNSSEC_Error('mail.ietf.org', 'AAAA', '194.191.40.84', 'DNSSEC Error for hostname mail.ietf.org
(AAAA) while asking 194.191.40.84. Error was: Unsupported qtype') of qtype AAAA looking up
mail.ietf.org
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q('mail.ietf.org', 'CNAME')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QN('mail.ietf.org', 'CNAME',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:48 2019 Debug: DNS query: QIP ('mail.ietf.org','CNAME','194.191.40.83',60)
Mon Feb 4 20:08:48 2019 Debug: DNS query: Q ('mail.ietf.org', 'CNAME', '194.191.40.83')
Mon Feb 4 20:08:48 2019 Debug: DNSSEC Response data([], , 0, 1800)
Mon Feb 4 20:08:48 2019 Debug: Received NODATA for domain mail.ietf.org type CNAME
Mon Feb 4 20:08:48 2019 Debug: No CNAME record(NoError) found for domain(mail.ietf.org)

Mon Feb  4 20:08:49 2019 Debug: DNS query: Q('_25._tcp.mail.ietf.org', 'TLSA')
Mon Feb 4 20:08:49 2019 Debug: DNS query: QN('_25._tcp.mail.ietf.org', 'TLSA',
'recursive_nameserver0.parent')
Mon Feb 4 20:08:49 2019 Debug: DNS query: QIP
('_25._tcp.mail.ietf.org','TLSA','194.191.40.83',60)
Mon Feb 4 20:08:49 2019 Debug: DNS query: Q ('_25._tcp.mail.ietf.org', 'TLSA', '194.191.40.83')
Mon Feb  4 20:08:49 2019 Debug: DNSSEC Response
data(['0301010c72ac70b745ac19998811b131d662c9ac69dbdbe7cb23e5b514b56664c5d3d6'], secure, 0,
1800)
Mon Feb  4 20:08:49 2019 Debug: DNS encache (_25._tcp.mail.ietf.org, TLSA, [(8496577312207991L,
0, 'SECURE', '0301010c72ac70b745ac19998811b131d662c9ac69dbdbe7cb23e5b514b56664c5d3d6')])
```

fail sample daneverify

[]> thinkbeyond.ch

```
INSECURE MX record(thinkbeyond-ch.mail.protection.outlook.com) found for thinkbeyond.ch
INSECURE MX record(thinkbeyond-ch.mail.protection.outlook.com) found. The command will still proceed.
INSECURE A record (104.47.9.36) found for MX(thinkbeyond-ch.mail.protection.outlook.com) in thinkbeyond.ch
Trying next A record (104.47.10.36) for MX(thinkbeyond-ch.mail.protection.outlook.com) in thinkbeyond.ch
INSECURE A record (104.47.10.36) found for MX(thinkbeyond-ch.mail.protection.outlook.com) in thinkbeyond.ch
DANE FAILED for thinkbeyond.ch
DANE verification completed.
```

mail_logs
Sample output from the execution of he danverify thinkbeyond.ch will populate the dns lookups

within the mail logs

```
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond.ch', 'MX')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond.ch', 'MX',
'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond.ch','MX','194.191.40.84',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond.ch', 'MX', '194.191.40.84')
Mon Feb  4 20:15:52 2019 Debug: DNSSEC Response data([(10, 'thinkbeyond-
ch.mail.protection.outlook.com.')], insecure, 0, 3600)
Mon Feb 4 20:15:52 2019 Debug: DNS encache (thinkbeyond.ch, MX, [(8502120882844461L, 0,
'INSECURE', (10, 'thinkbeyond-ch.mail.protection.outlook.com'))])
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond-ch.mail.protection.outlook.com', 'A')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond-ch.mail.protection.outlook.com', 'A',
'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','A','194.191.40.83',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com', 'A',
'194.191.40.83')
Mon Feb  4 20:15:52 2019 Debug: DNSSEC Response data(['104.47.9.36', '104.47.10.36'], insecure,
0, 10)
Mon Feb 4 20:15:52 2019 Debug: DNS encache (thinkbeyond-ch.mail.protection.outlook.com, A,
[(8497631700844461L, 0, 'INSECURE', '104.47.9.36'), (8497631700844461L, 0, 'INSECURE',
'104.47.10.36')])
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond-ch.mail.protection.outlook.com',
'AAAA')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond-ch.mail.protection.outlook.com',
'AAAA', 'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','AAAA','194.191.40.84',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com',
'AAAA', '194.191.40.84')
Mon Feb 4 20:15:52 2019 Debug: DNSSEC Response data([], , 0, 32768)
Mon Feb 4 20:15:52 2019 Debug: Received NODATA for domain thinkbeyond-
ch.mail.protection.outlook.com type AAAA
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QN('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME', 'recursive_nameserver0.parent')
Mon Feb 4 20:15:52 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','CNAME','194.191.40.83',60)
Mon Feb 4 20:15:52 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME', '194.191.40.83')
Mon Feb 4 20:15:53 2019 Warning: Received an invalid DNS Response: SERVER FAILED to IP
194.191.40.83 looking up thinkbeyond-ch.mail.protection.outlook.com
Mon Feb 4 20:15:53 2019 Debug: DNS query: QIP ('thinkbeyond-
ch.mail.protection.outlook.com','CNAME','194.191.40.84',60)
Mon Feb 4 20:15:53 2019 Debug: DNS query: Q ('thinkbeyond-ch.mail.protection.outlook.com',
'CNAME', '194.191.40.84')
Mon Feb 4 20:15:54 2019 Warning: Received an invalid DNS Response: SERVER FAILED to IP
194.191.40.84 looking up thinkbeyond-ch.mail.protection.outlook.com
Mon Feb 4 20:15:54 2019 Debug: No CNAME record() found for domain(thinkbeyond-
ch.mail.protection.outlook.com)
```

Gerelateerde informatie

- ESA-gebruikershandleidingen
- Releaseopmerkingen van ESA
- ESR CLI-handleidingen