DANE pour l'appliance de sécurité de la messagerie

Contenu

Introduction

Ce document décrit la mise en oeuvre de DANE pour le flux de courrier sortant ESA.

Conditions préalables

Connaissance générale des concepts et de la configuration de l'ESA.

Exigences relatives à la mise en oeuvre de DANE :

- Résolution DNS compatible DNSSEC
- ESA avec AsyncOS 12.0 ou version ultérieure

Informations générales

DANE a été introduit dans ESA 12 pour la validation du courrier sortant.

Authentification DNS des entités nommées (DANE).

- DANE est un protocole de sécurité Internet permettant aux certificats numériques X.509 d'être liés aux noms de domaine à l'aide de DNSSEC. (RFC 6698)
- DNSSEC est un ensemble de spécifications IETF pour sécuriser les enregistrements DNS à

l'aide de la cryptographie à clé publique. (explication très élémentaire. RFC 4033, RFC 4034 et RFC 4035)

Considérations relatives à la mise en oeuvre

Vérifiez que le ESA utilise un résolveur DNS compatible dnssec.

La mise en oeuvre de DANE nécessite la capacité DNS permettant d'effectuer des requêtes Dnssec/DANE.

Pour tester la fonctionnalité DANE DNS ESA, un test simple peut être effectué à partir de la connexion CLI ESA.

La commande CLI 'daneverify' exécute les requêtes complexes pour vérifier si un domaine est capable de passer la vérification DANE.

La même commande peut être utilisée avec un domaine valide connu pour confirmer la capacité de l'ESA à résoudre les requêtes dnssec.

'ietf.org' est une source mondialement connue. L'exécution de la commande cli 'daneverify' permet de vérifier si le résolveur DNS est compatible DANE ou non.

PASS VALIDE : RÉSULTATS DU SERVEUR DNS DANE CAPABLE « DANE SUCCESS » POUR ietf.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.
```

ÉCHEC NON VALIDE : RÉSULTATS DE BOGUS DU SERVEUR DNS CAPABLE NON DANE POUR ietf.org

```
> daneverify ietf.org

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

ÉCHEC VALIDE : daneverify cisco.com > cisco n'a pas mis en oeuvre DANE. Il s'agit du résultat attendu d'un résolveur compatible dnssec.

```
> 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.
```

Si les tests ci-dessus sont « VALIDE », ils fonctionnent :

- Une approche prudente consisterait à tester chaque domaine avant d'ajouter un profil pour le domaine.
- Une approche plus agressive consisterait à configurer DANE sur le profil des contrôles de destination par défaut et à voir qui réussit/échoue.

La Direction du courrier détermine si DANE vérifiera.

Les stratégies de flux de groupe d'expéditeurs/de courrier dont l'action « RELAY » est configurée effectueront la vérification DANE.

Les stratégies de flux de groupe d'expéditeurs/de courrier dont l'action ACCEPT est configurée n'effectueront PAS la vérification DANE.

> **Attention** : Si le SEEE a le contrôle de destination DANE activé sur la **stratégie par défaut**, **il existe un risque d'échec de livraison.** Si un domaine appartenant à l'interne, tel que ceux répertoriés dans le RAT, passe par les stratégies de flux de courrier RELAY et ACCEPT, associées à la présence d'une route SMTP pour le domaine.

Routes SMTP

DANE échouera sur les routes SMTP, sauf si l'hôte de destination est configuré sur USEDNS.

DANE Opportunistic ne livrera pas les messages, les contenant dans la file d'attente de remise jusqu'à l'expiration du compteur de profil de renvoi.

Pourquoi ? La vérification DANE est ignorée car une route SMTP serait une modification de la destination réelle et pourrait ne pas utiliser correctement DNS.

Solution : Créer des profils de contrôle de destination pour désactiver explicitement la vérification DANE pour les domaines contenant des routes SMTP

DANE opportuniste ou DANE obligatoire

Les recherches suivantes sont effectuées lors de la vérification DANE.

Chaque vérification alimente le contenu pour effectuer la vérification suivante.

- La recherche d'enregistrement MX vérifie si »> est sécurisé, non sécurisé, biogue

- Une recherche d'enregistrement vérifie si »> Secure Insecure > Bogus
- La recherche d'enregistrement TLSA vérifie si »> Secure, Insecure, Bogus, NXDOMAIN
- Vérification du certificat » Réussite, échec

Sécurisé :

- DNS a vérifié la présence d'un enregistrement sécurisé contenant un RRSIG validé signé RRSIG DS et DNSKEY, dans la chaîne de confiance.

Insécurisé :

- DNS détermine que le domaine ne contient aucun enregistrement compatible dnssec.

Bogus :

- Les entrées dnssec incomplètes mais présentes peuvent échouer à la vérification.
- Enregistrements non valides en raison d'une clé expirée.
- Enregistrement ou clé manquant dans la chaîne de confiance.

NXDOMAINE

- Aucun enregistrement trouvé dans DNS.

Une combinaison de la vérification des enregistrements ci-dessus et des résultats de la vérification déterminera la réussite du DANE | Échec du DANE | Reprise DANE vers TLS. »

Par exemple : si aucun RRSIG n'est envoyé pour l'enregistrement MX de example.com, la zone parent (.com) est vérifiée pour voir si example.com a un enregistrement DNSKEY, indiquant que example.com doit signer ses enregistrements. Cette validation se poursuit jusqu'à la fin de la chaîne d'approbation avec la vérification de clé de la zone racine (.). Elle est atteinte et les clés de la zone racine correspondent aux attentes de l'ESA (valeurs codées en dur sur l'ESA, qui est automatiquement mise à jour sur la base de RFC5011).

DANE OBLIGATOIRE

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 OBLIGATOIRE

Remarque: DANE OPPORTUNISTIC **NE SE COMPORTE PAS COMME TLS PRÉFÉRÉ**. La partie ACTION du tableau ci-dessous donne les résultats DANE FAIL, ne livrera ni obligatoire ni opportuniste. Les messages resteront dans la file d'attente de remise jusqu'à ce que le compteur expire, puis la remise se termine.

DANE OPPORTUNISTE

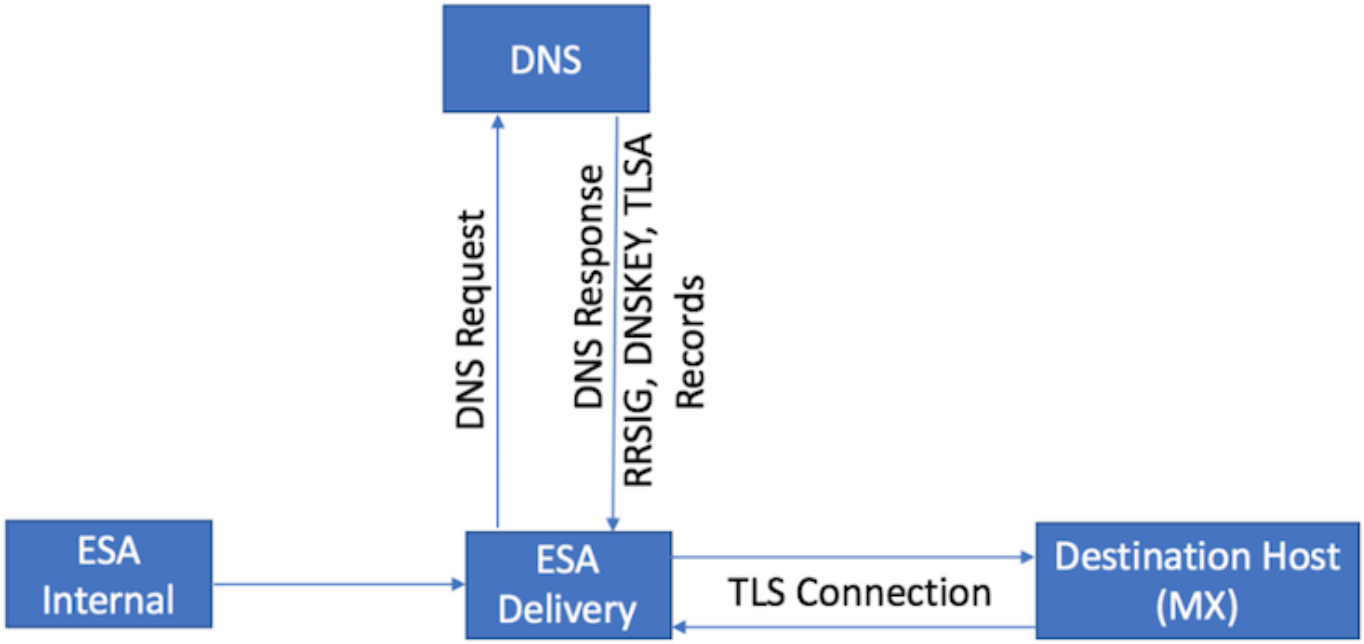
MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed →	DANE Fail
Secure	Secure	Insecure		Fallback to opportunistic TLS flow
Secure	secure	NXDOMAIN		Fallback to opportunisticTLS flow
Secure	Secure	Bogus	→	DANE Fail
Secure	Insecure	Mail 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 OPPORTUNISTE

Activer DANE sur plusieurs environnements d'appareils

La figure suivante illustre le flux de travail lorsque vous activez DANE dans un environnement d'appliances multiples.

Si l'environnement comporte plusieurs couches d'appliances ESA, l'une pour l'analyse et l'autre pour la remise des messages Assurez-vous que le DANE est configuré uniquement sur l'appliance qui se connecte directement aux destinations externes.



Conception Multi-ESA. DANE configuré sur l'ESA de livraison

Gestion de plusieurs restaurateurs DNS

Si un ESA a plusieurs résolveurs DNS configurés, quelques-uns qui prennent en charge DNSSEC quelques-uns qui ne prennent pas en charge DNSSEC, Cisco recommande de configurer les résolveurs compatibles DNSSEC avec une priorité plus élevée (valeur numérique inférieure), afin d'éviter les incohérences.

Cela empêche le résolveur non-DNSSEC de classer le domaine de destination prenant en charge DANE comme 'Bogus'.

Gestion du serveur DNS secondaire

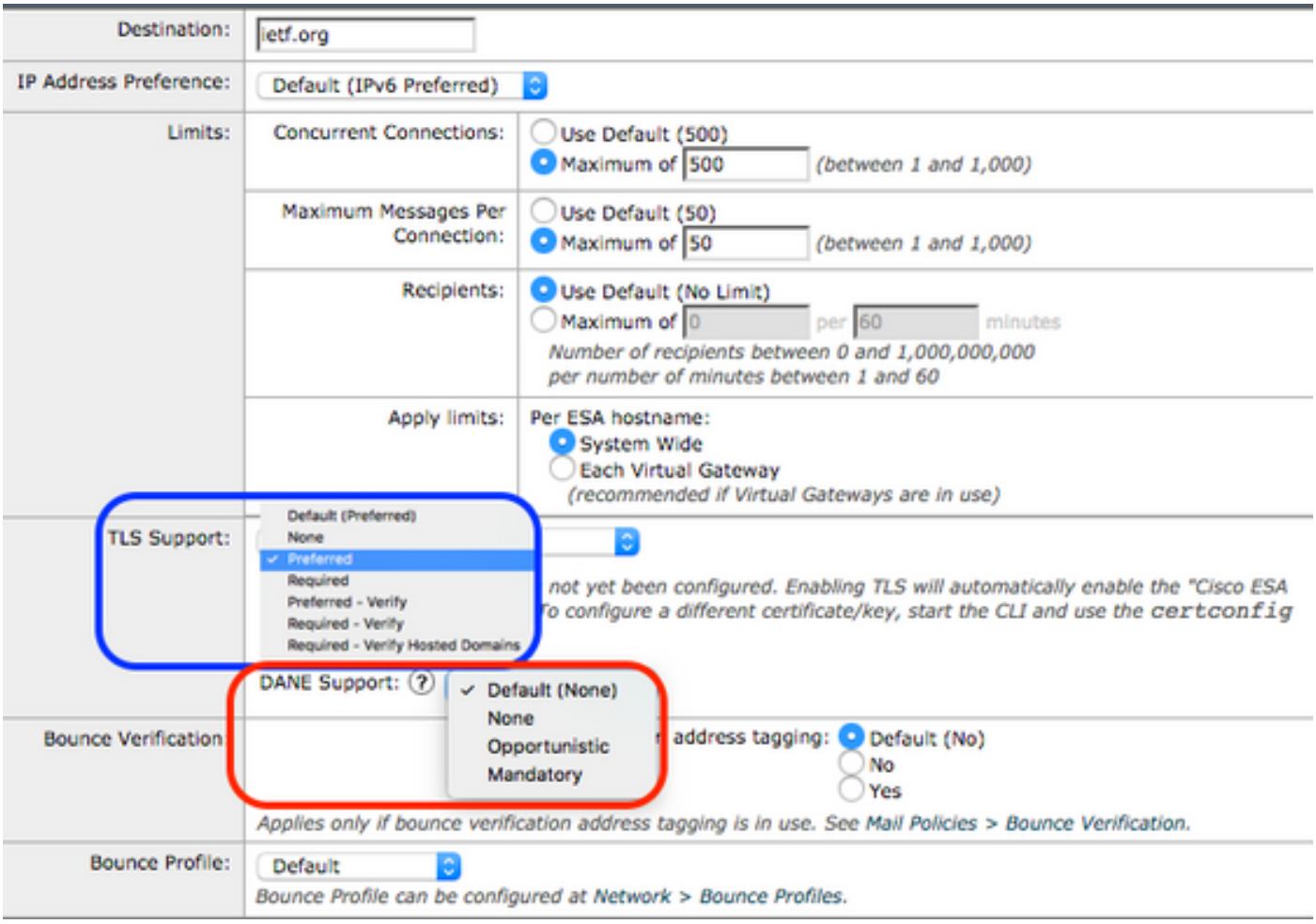
Lorsque le résolveur DNS n'est pas accessible, le DNS revient au serveur DNS secondaire. Si vous ne configurez pas DNSSEC sur le serveur DNS secondaire, les enregistrements MX pour les domaines de destination compatibles DANE sont classés en tant que Bogus. Cela affecte la remise des messages indépendamment des paramètres DANE (Opportuniste ou Obligatoire). Cisco vous recommande d'utiliser un résolveur DNSSEC secondaire.

Configuration

Configurez DANE pour le flux de courrier sortant.

1. Naviguez jusqu'à > Politiques de messagerie > Contrôles de destination > Ajouter une destination
2. Remplissez la partie supérieure du profil selon vos préférences.
3. Prise en charge TLS : **doit être défini sur « TLS Preferred » | Préféré - Vérifier | Requis | Obligatoire - Vérifier| Obligatoire - Vérifier le domaine hébergé**. »
4. Une fois la prise en charge TLS activée, la prise en charge DANE : le menu déroulant devient actif.
5. **Support DANE : options : « Aucun » | Opportuniste | Obligatoire.**

6. Une fois l'option Support DANE terminée, envoyez et validez les modifications.



Profil de contrôle de destination - Vérification DANE

Vérifier le succès de DANE

État de livraison

Surveillez le rapport WebUI « Delivery Status » pour toute accumulation non intentionnelle de domaines de destination, potentiellement due à une défaillance DANE.

Effectuez cette opération avant d'activer le service, puis périodiquement pendant plusieurs jours pour assurer le succès continu.

ESA WebUI > Monitor > Delivery Status > cochez la colonne « Destinataires actifs ».

Journaux de messagerie

Journaux de messagerie par défaut au niveau des informations pour le niveau du journal.

Les journaux de messagerie affichent des indicateurs très subtils pour les messages négociés par DANE.

La négociation TLS finale sortante inclura une sortie légèrement modifiée pour inclure le domaine à la fin de l'entrée de journal.

L'entrée du journal inclura « protocole de réussite TLS » suivi de la version/chiffrement TLS « pour domain.com ».

La magie est dans le « for » :

```
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
```

Débogage des journaux de messagerie

Les journaux de messagerie personnalisés au niveau de débogage afficheront des recherches DANE et dnssec complètes, la négociation attendue, des parties de la vérification qui réussissent/échouent et un indicateur de succès.

> **Remarque: Les journaux de messagerie configurés pour la journalisation du niveau de débogage peuvent consommer des ressources excessives sur un ESA en fonction de la charge et de la configuration du système.**

Les journaux de messagerie configurés pour la journalisation du niveau de débogage peuvent consommer des ressources excessives sur un ESA en fonction de la charge et de la configuration du système.

Les journaux de messagerie ne sont généralement PAS gérés au niveau de débogage pendant de longues périodes.

Les journaux de niveau de débogage peuvent générer un volume énorme de journaux de messagerie en peu de temps.

Une pratique fréquente consiste à créer un abonnement de journal supplémentaire pour mail_logs_d et à définir la journalisation pour DEBUG.

L'action empêche l'impact sur les journaux de messagerie existants et permet la manipulation du volume de journaux mis à jour pour l'abonnement.

Pour contrôler le volume des journaux créés, limitez le nombre de fichiers à conserver à un nombre plus petit, par exemple 2-4 fichiers.

Lorsque la surveillance, la période d'essai ou le dépannage sont terminés, désactivez le journal.

Les journaux de messagerie définis pour le niveau de débogage affichent une sortie DANE très détaillée :

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)
```

Informations connexes

- Guides d'utilisation ESA
- Notes de version ESA

- Guides de référence de l'interface CLI ESA