DANE for Eメールセキュリティアプライアンス

目次

はじめに

このドキュメントでは、ESAアウトバウンドメールフローのDANE実装について説明します。

前提条件

ESAの概念と設定に関する一般的な知識。

DANEを実装するための要件：

- DNSSEC対応DNSリゾルバ
- AsyncOS 12.0以降のESA

背景説明

DANEは、送信メール検証のためにESA 12に導入されました。

名前付きエンティティ(DANE)のDNSベース認証。

- DANEは、X.509デジタル証明書をDNSSECを使用してドメイン名にバインドできるようにするインターネットセキュリティプロトコルです。(RFC 6698)
- DNSSECは、公開キー暗号化を使用してDNSレコードを保護するためのIETF仕様のコレクションです。(非常に基本的な説明。RFC 4033、RFC 4034、およびRFC 4035)

実装に関する考慮事項

ESAがdnssec対応DNSリゾルバを使用していることを確認します。

DANEを実装するには、dnssec/DANEクエリを実行するDNS機能が必要です。

ESA DNS DANE機能をテストするには、ESA CLIログインから簡単なテストを実行できます。

CLIコマンド「daneverify」は、複雑なクエリを実行して、ドメインがDANE検証を通過できるかどうかを確認します。

正常なドメインと同じコマンドを使用して、ESAがdnssecクエリを解決できることを確認できます。

「ietf.org」は世界的に知られている情報源です。cliコマンド「daneverify」を実行すると、DNSリゾルバがDANEに対応しているかどうかが確認されます。

有効なパス：IETF.orgのDANE対応DNSサーバ「DANE SUCCESS」の結果

```
> 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.
```

無効な失敗：IETF.orgのDANE非対応DNSサーバ「BOGUS」の結果

```
> daneverify ietf.org

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

有効な失敗：daneverify cisco.com > cisco has not implemented DANE.これは、dnssec対応リゾルバの予想される結果です。

```
> 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.
```
上記のテストが「VALID」の場合：

- 慎重なアプローチとして、ドメインのプロファイルを追加する前に各ドメインをテストします。
- よりアグレッシブなアプローチは、デフォルトの宛先制御プロファイルでDANEを設定し、誰が通過/失敗するかを確認することです。

メールの方向は、DANEが確認するかどうかを決定します。

「RELAY」アクションが設定されている送信者グループ/メールフローポリシーは、DANE検証を実行します。

「ACCEPT」アクションが設定されている送信者グループ/メールフローポリシーは、DANE検証を実行しません。

> **注意**：ESAのデフォルトポリシーで宛先制御「DANE」が有効になっている場**合、配信**に失敗**するリスクがあります。** RATにリストされているような内部所有ドメインは、RELAYとACCEPTの両方のメールフローポリシーを通過し、ドメインのSMTPルートの存在を組み合わせます。

SMTPルート

「宛先ホスト」が「USEDNS」に設定されていない限り、DANEはSMTPルートで失敗します。

DANE Opportunisticは、バウンスプロファイルタイマーが期限切れになるまで、メッセージを配信キューに含めて、メッセージを配信しません。

これは、なぜですか。DANE検証は、SMTPルートが真の宛先の変更であり、DNSを正しく使用しない可能性があるためスキップされます。

ソリューション：SMTPルートを含むドメインのDANE検証を明示的に無効にする宛先制御プロファイルの作成

DANE OpportunisticまたはDANE Mandatory

次のルックアップは、DANE検証時に実行されます。

各検証は、コンテンツをフィードして、後続の検証を実行します。

- MXレコードのルックアップは、>>>セキュア、セキュア、非セキュア、不正を検証します
- レコード検索は、>>> Secure Insecure > Bogusかどうかを確認します
- TLSAレコードのルックアップは、>>>セキュア、セキュア、非セキュア、偽、NXDOMAINかどうかを確認します
- 証明書の確認>>成功、失敗

セキュア：

- DNSは、RRSIG検証済みの署名付きRRSIG DSとDNSKEYを含む安全なレコードが存在することを確認し、信頼チェーンを確立しました。

Insecure:

- DNSは、ドメインにdnssec対応レコードがないことを確認します。

偽：

- 不完全ですが、現在のdnssecエントリは検証に失敗する可能性があります。
- キーの有効期限が切れているため、無効なレコードです。
- 信頼のチェーンにレコードまたはキーがありません。

NXDOMAIN

- DNSにレコードが見つかりません。

上記のレコードチェックと検証結果の組み合わせにより、「DANE Success | DANE Fail | DANEがTLSにフォールバックします。

例：example.comのMXレコードにRRSIGが送信されない場合は、親ゾーン(.com)がチェックされ、example.comにDNSKEYレコードが含まれているかどうかが確認されます。これは、example.comがレコードに署名する必要があることを示します。この検証は、ルートゾーン(.)キー検証を使用してトラストチェーンを終了し続け、ルートゾーンのキーはESAが期待するキー（RFC5011に基づいて自動更新されるESAのハードコード値）と一致します。

DANE必須

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必須

注：DANE OPPORTUNISTICは**TLSの推奨動作ではありません**。次のグラフのACTION部分は、DANE FAILの結果であり、MandatoryまたはOpportunisticのいずれについても提供されません。メッセージは、タイマーが時間切れになるまで配信キューに残り、配信が終了します。

日和見主義

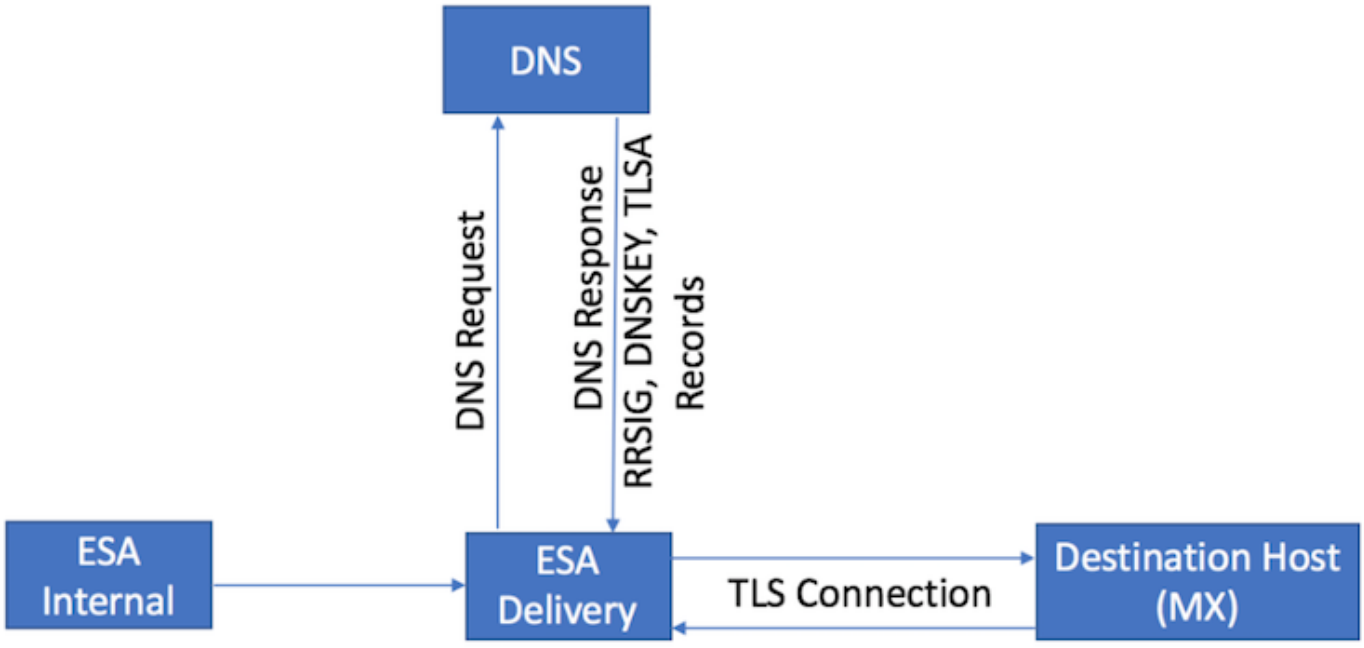
MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed →	DANE Fail
Secure	Secure	Insecure		Fallback to opportunistic TLS flow
Secure	secure	NXDOMAIN		Fallback to opportunisticTLS flow
Secure	Secure	Bogus	→	DANE Fail
Secure	Insecure	Mail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

日和見主義

複数アプライアンス環境でのDANEの有効化

次の図は、複数のアプライアンス環境でDANEを有効にする場合のワークフローを示しています。

環境にESAアプライアンスの複数のレイヤがある場合、1つはスキャン用で、もう1つはメッセージ配信用です。DANEは、外部の宛先に直接接続するアプライアンスでのみ設定してください。



マルチESA設計配信ESAで設定されたDANE

複数のDNSリゾルバの管理

ESAに複数のDNSリゾルバが設定されている場合、DNSSECをサポートするDNSリゾルバと、DNSSECをサポートしないDNSSEC対応のリゾルバを高い優先順位（数値が低い）で設定することをお勧めします。

これにより、DNSSEC非対応リゾルバがDANEをサポートする宛先ドメインを「Bogus」に分類することを防止できます。

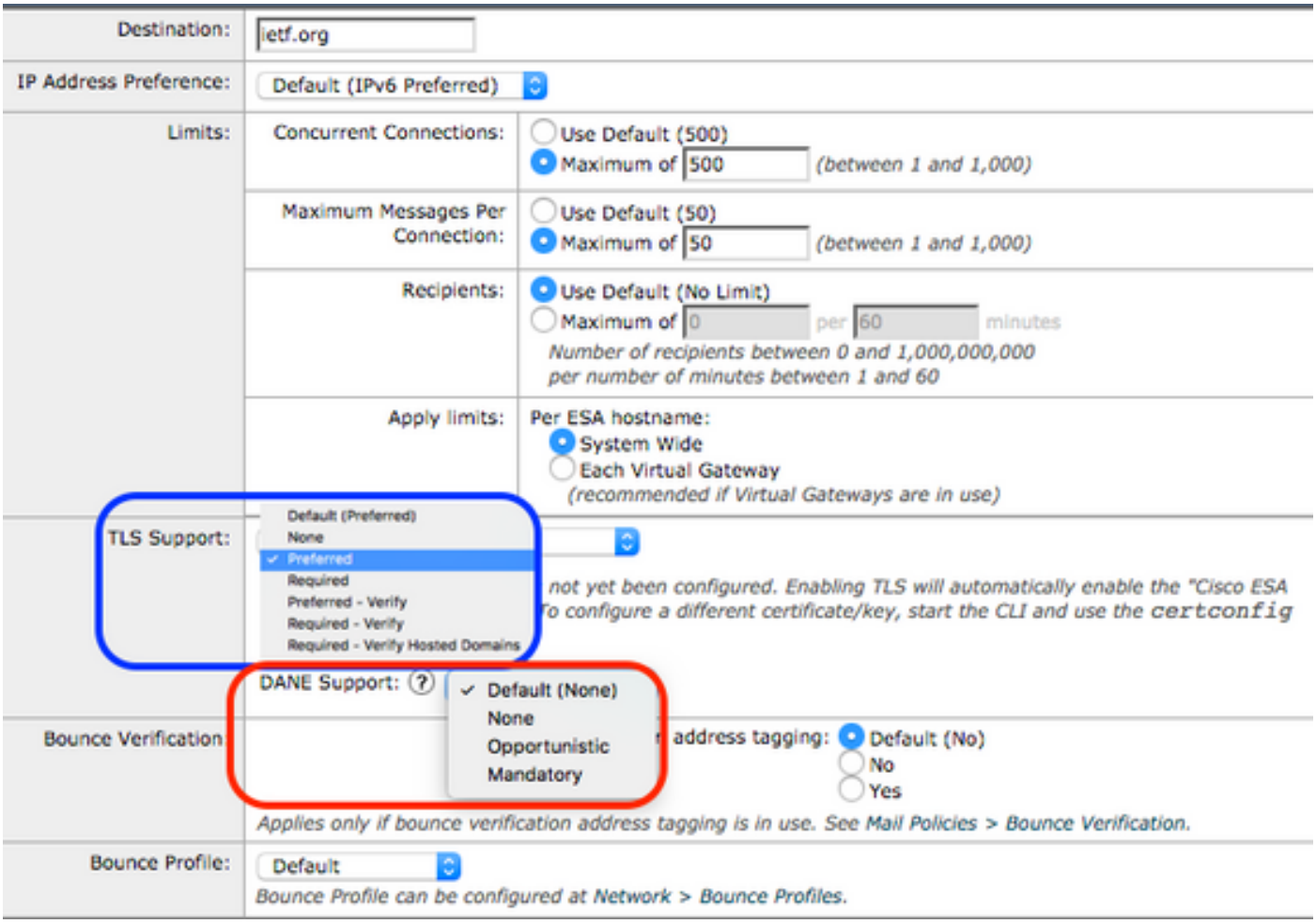
セカンダリDNSサーバの管理

DNSリゾルバに到達できない場合、DNSはセカンダリDNSサーバにフォールバックします。セカンダリDNSサーバでDNSSECを設定しない場合、DANE対応の宛先ドメインのMXレコードは「Bogus」に分類されます。 これは、DANE設定（OpportunisticまたはMandatory）に関係なく、メッセージ配信に影響します。 セカンダリDNSSEC対応リゾルバを使用することを推奨します。

コンフィギュレーション

アウトバウンドメールフロー用にDANEを設定します。

1. Webuiに移動> [Mail Policies] > [Destination Controls] > [Add Destination]に移動
2. プロファイルの上部に設定を入力します。
3. TLSサポート：**[TLS Preferred]に設定する必要があります |優先 – 確認 |必須 |必須 – 確認|必須 – ホステッドドメインを確認**します。
4. TLSサポートが有効になると、DANEサポート：ドロップダウンメニューがアクティブになります。
5. **DANEサポート：オプションには「なし」が含まれます | Opportunistic |必須。**
6. DANE Supportオプションが完了したら、変更を送信して確定します。



宛先制御プロファイル – DANEの確認

DANEの成功の確認

配信ステータス

WebUIの「Delivery Status」レポートで、DANEの障害が原因で発生する可能性がある、意図しない宛先ドメインの構築を監視します。

サービスを有効にする前に、これを数日間定期的に実行して、継続的な成功を保証します。

[ESA WebUI] > [Monitor] > [Delivery Status] > [Active Recipients]列を確認します。

メールログ

ログレベルの情報レベルのデフォルトメールログ。

メールログには、DANEが正常にネゴシエートしたメッセージの非常に微妙なインジケータが表示されます。

最後のTLSネゴシエーションアウトバウンドには、ログエントリの最後にドメインを含むように若干変更された出力が含まれます。

ログエントリには、「TLS success protocol」の後にTLSバージョン/暗号「for domain.com」が続きます。

魔法は「for」にあります。

```
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
```

メールログのデバッグ

デバッグレベルのカスタムメールログには、DANEとdnssecの完全なルックアップ、ネゴシエーションが予想され、チェックの一部が合格/失敗し、成功インジケータが表示されます。

> **注：デバッグレベルのロギング用に設定されたメールログは、システムの負荷と設定に応じて、ESAで過剰なリソースを消費する場合があります。**

デバッグレベルのロギング用に設定されたメールログは、システムの負荷と設定に応じて、ESAで過剰なリソースを消費する場合があります。

メールログは通常、長時間デバッグレベルで維持されません。

デバッグレベルのログは、短時間で大量のメールログを生成する可能性があります。

mail_logs_d用に追加のログサブスクリプションを作成し、DEBUG用にロギングを設定することが頻繁に行われます。

このアクションは、既存のmail_logsへの影響を防止し、サブスクリプションに保持されているログのボリュームを操作できるようにします。

作成される口グのボリュームを制御するには、保持するファイルの数を2 ~ 4ファイルなどの少ない数に制限します。

モニタリング、トライアル期間、またはトラブルシューティングが完了したら、ログを無効にします。

デバッグレベルに設定されたメールログは、非常に詳細なDANE出力を示します。

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)
```

関連情報

- ESAユーザガイド
- ESAリリースノート
- ESA CLIリファレンスガイド