DANE für E-Mail Security Appliance

Inhalt

Einführung

Dieses Dokument beschreibt die DANE-Implementierung für den E-Mail-Fluss der ESA.

Voraussetzungen

Allgemeine Kenntnisse der ESA-Konzepte und -Konfiguration.

Anforderungen für die DANE-Implementierung:

- DNS-Resolver mit DNS-SSEC-Unterstützung
- ESA mit AsyncOS 12.0 oder höher

Hintergrundinformationen

DANE wurde für die Validierung von ausgehenden E-Mails in ESA 12 eingeführt.

DNS-basierte Authentifizierung benannter Entitäten (DANE).

- DANE ist ein Internetsicherheitsprotokoll, das es X.509-digitalen Zertifikaten erlaubt, mit DNSSEC an Domänennamen gebunden zu sein. (RFC 6698)
- DNSSEC ist eine Sammlung von IETF-Spezifikationen zum Sichern von DNS-Datensätzen mithilfe von Public-Key-Verschlüsselung. (Sehr elementare Erklärung. RFC 4033, RFC 4034 und RFC 4035)

Überlegungen zur Implementierung

Überprüfen Sie, ob die ESA einen DNS-Resolver mit dnssec-Funktion verwendet.

Für die DANE-Implementierung ist die DNS-Funktion zum Durchführen von Dnssec-/DANE-Abfragen erforderlich.

Um die ESA DNS DANE-Funktion zu testen, kann ein einfacher Test mithilfe der CLI-Anmeldung der ESA durchgeführt werden.

Der CLI-Befehl 'daneverify' führt die komplexen Abfragen aus, um zu überprüfen, ob eine Domäne die DANE-Überprüfung übergeben kann.

Der gleiche Befehl kann mit einer zweifelsfrei funktionierenden Domäne verwendet werden, um die ESA-Fähigkeit zum Auflösen von dnssec-Abfragen zu bestätigen.

'ietf.org' ist eine weltweit bekannte Quelle. Durch Ausführen des CLI-Befehls 'daneverify' wird überprüft, ob der DNS-Resolver DANE-fähig ist.

GÜLTIGE BESTANDTEIL: DANE CAPABLE DNS SERVER "DANE ERFOLGREICH" ERGEBNISSE FÜR 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.
```

UNGÜLTIGER AUSFALL: NICHT DANE FÄHIGE DNS-SERVER "BOGUS"-ERGEBNISSE FÜR ietf.org

```
> daneverify ietf.org

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

GÜLTIGER AUSFALL: daneverify cisco.com > cisco hat DANE nicht implementiert. Dies ist das erwartete Ergebnis eines dnssec-fähigen Resolvers.

```
> 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.
```

Wenn die oben genannten Tests "GÜLTIG" funktionieren:

- Ein vorsichtiger Ansatz besteht darin, jede Domäne vor dem Hinzufügen eines Profils für die Domäne zu testen.
- Ein aggressiverer Ansatz wäre die Konfiguration von DANE im Profil der Standard-Zielsteuerelemente und die Überprüfung, wer die Prüfung besteht/versagt.

Die E-Mail-Richtung bestimmt, ob DANE überprüfen wird.

Absendergruppe/Mail Flow-Richtlinien, für die die Aktion "RELAY" konfiguriert ist, führen eine DANE-Überprüfung durch.

Absendergruppe/Mail Flow-Richtlinien, für die die Aktion "ACCEPT" konfiguriert ist, führen KEINE DANE-Überprüfung durch.

> **Vorsicht:** Wenn die Zielsteuerelemente "DANE" für die ESA in der **Standardrichtlinie** aktiviert sind, **besteht das Risiko einer fehlgeschlagenen Zustellung.** Wenn eine interne Domäne, wie die im RAT aufgelisteten Domänen, die E-Mail-Flow-Richtlinien für RELAY und ACCEPT durchläuft, kombiniert mit dem Vorhandensein einer SMTP-Route für die Domäne.

SMTP-Routen

DANE schlägt auf SMTP-Routen fehl, es sei denn, der "Ziel-Host" ist für "USEDNS" konfiguriert.

DANE Opportunistic liefert die Nachrichten, die sie in der Delivery Queue enthalten, erst dann, wenn der Bounce-Profil-Timer abläuft.

Warum? Die DANE Verifizierung wird übersprungen, da eine SMTP-Route eine Änderung des echten Ziels darstellt und möglicherweise DNS nicht korrekt verwendet.

Lösung: Erstellen von Zielsteuerungsprofilen zum expliziten Deaktivieren der DANE Verifizierung für Domänen, die SMTP-Routen enthalten

DANE Opportunistisch oder DANE Obligatorisch

Die folgenden Suchvorgänge werden während der DANE-Überprüfung ausgeführt.

Bei jeder Überprüfung werden Inhalte zur anschließenden Überprüfung eingesendet.

- Die MX-Datensatzsuche verifiziert, ob >>> Sicher, unsicher, Bogus
- Eine Datensatzsuche überprüft, ob >>> Sicher unsicher > Bogus
- Die TLSA-Datensatzsuche überprüft, ob >>> Sicher, unsicher, Bogus, NXDOMAIN
- Zertifikatverifizierung >> Erfolgreich, Fehler

Sicher:

- DNS hat das Vorhandensein eines sicheren Datensatzes überprüft, der ein RSIG-validiertes signiertes RSIG DS und DNSKEY (oben in der Vertrauenskette) enthält.

Unsicher:

- DNS bestimmt, dass die Domäne keine dnssec-fähigen Datensätze enthält.

Bogus:

- Unvollständig, aber die vorhandenen DNS-Einträge können nicht überprüft werden.
- Ungültige Datensätze aufgrund eines abgelaufenen Schlüssels.
- Fehlender Datensatz oder Schlüssel in der Vertrauenskette.

NXDOMÄNE

- Im DNS wurde kein Datensatz gefunden.

Eine Kombination aus der oben beschriebenen Überprüfung und den Prüfergebnissen bestimmt "DANE Success" | DANE FEHLER | DANE Fallback to TLS."

Beispiel: Wenn kein RRSIG für den MX-Datensatz von example.com gesendet wurde, wird die übergeordnete Zone (.com) überprüft, um festzustellen, ob example.com über einen DNSKEY-Datensatz verfügt. Dies bedeutet, dass example.com seine Datensätze signieren soll. Diese Validierung setzt die Kette der Vertrauensbeendigung fort, wobei die Schlüsselüberprüfung für die Root-Zone (.) erreicht wird und die Schlüssel der Root-Zone mit den Erwartungen der ESA übereinstimmen (hartcodierte Werte für die ESA, die basierend auf RFC5011 automatisch aktualisiert werden).

DANE OBDATORY

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 OBDATORY

Hinweis: DANE OPPORTUNISTIC **VERHÄLT SICH NICHT WIE TLS BEVORZUGT**. Der Teil

"AKTION" in der unten stehenden Tabelle zeigt die Ergebnisse DANE FEHL, wird nicht liefern für Obligatorisch oder Opportunistisch. Die Nachrichten verbleiben bis zum Ablauf des Timers in der Zustellungswarteschlange, und die Zustellung wird beendet.

DÄNE-OPPORTUNISTISCH

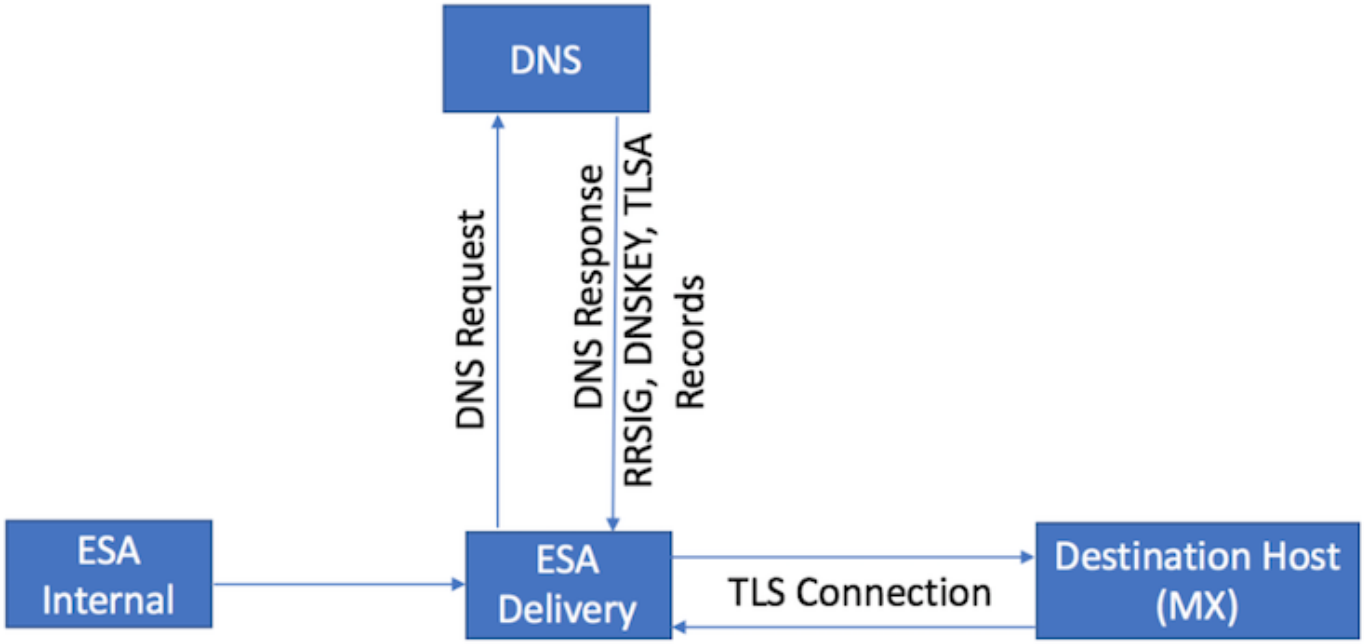
MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed →	DANE Fail
Secure	Secure	Insecure		Fallback to opportunistic TLS flow
Secure	secure	NXDOMAIN		Fallback to opportunisticTLS flow
Secure	Secure	Bogus	→	DANE Fail
Secure	Insecure	Mail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

DÄNE-OPPORTUNISTISCH

DANE in einer Umgebung mit mehreren Appliances aktivieren

Die folgende Abbildung zeigt den Workflow, in dem DANE in einer Umgebung mit mehreren Appliances aktiviert wird.

Wenn die Umgebung über mehrere Ebenen von ESA-Appliances verfügt, eine für das Scannen und eine andere für die Nachrichtenübermittlung. Stellen Sie sicher, dass DANE nur auf der Appliance konfiguriert wird, die direkt mit den externen Zielen verbunden ist.



Design mit mehreren ESAs. DANE auf der Delivery ESA konfiguriert

Verwalten mehrerer DNS-Auflösungen

Wenn für eine ESA mehrere DNS-Resolver konfiguriert sind, einige wenige, die DNSSEC unterstützen und DNSSEC nicht unterstützen, empfiehlt Cisco, die DNSSEC-fähigen Resolver mit einer höheren Priorität (Lower Numeric Value) zu konfigurieren, um Inkonsistenzen zu vermeiden.

Dies verhindert, dass der Nicht-DNSSEC-fähige Resolver die Zieldomäne, die DANE unterstützt, als 'Bogus' klassifiziert.

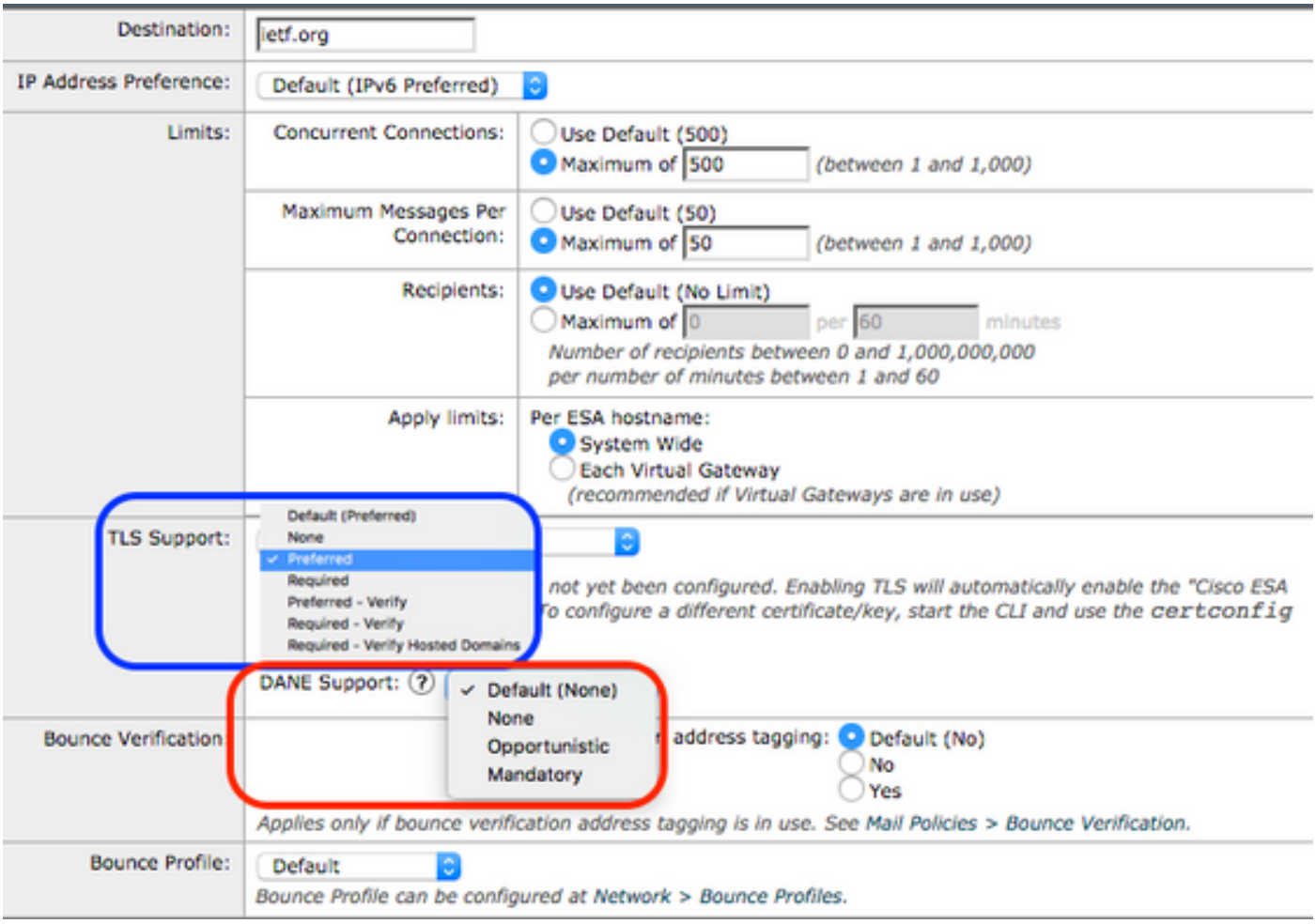
Verwalten des sekundären DNS-Servers

Wenn der DNS-Resolver nicht erreichbar ist, greift der DNS auf den sekundären DNS-Server zurück. Wenn Sie DNSSEC nicht auf dem sekundären DNS-Server konfigurieren, werden die MX Records für DANE-fähige Zieldomänen als "Bogus" klassifiziert. Dies wirkt sich unabhängig von den DANE-Einstellungen (Opportunistisch oder Obligatorisch) auf die Nachrichtenübermittlung aus. Cisco empfiehlt die Verwendung eines sekundären DNSSEC-fähigen Resolvers.

Konfiguration

Konfigurieren Sie DANE für den ausgehenden E-Mail-Fluss.

1. Navigieren Sie zu > Mail-Policys > Zielsteuerelemente > Ziel hinzufügen.
2. Füllen Sie den oberen Teil des Profils entsprechend Ihrer Präferenz aus.
3. TLS-Unterstützung: **muss auf "TLS Preferred" gesetzt werden. | Bevorzugt - Verifizieren | Erforderlich | Erforderlich - Verifizieren| erforderlich - Überprüfen der gehosteten Domäne**."
4. Sobald der TLS-Support aktiviert ist, bietet DANE Support: Das Dropdown-Menü wird aktiviert.
5. **DANE-Unterstützung: Optionen enthalten: Keine | Opportunistisch | Obligatorisch.**
6. Nach Abschluss der DANE Support-Option können Sie Änderungen senden und bestätigen.



Zielsteuerungsprofil - DANE Verifizieren

DANE erfolgreich verifizieren

Zustellungsstatus

Überwachen Sie den WebUI "Delivery Status"-Bericht für alle unbeabsichtigten Zugriffe auf Zieldomänen, möglicherweise aufgrund von DANE Failure.

Führen Sie diese Schritte vor der Aktivierung des Services durch. Anschließend können Sie in regelmäßigen Abständen mehrere Tage verbringen, um den Fortbestand des Services sicherzustellen.

ESA WebUI > Monitor > Delivery Status > Check the "Active Recipients" (Aktive Empfänger) column.

Mail-Protokolle

Die Standard-E-Mail-Protokolle befinden sich auf der Informations-Ebene für die Protokollebene.

Die E-Mail-Protokolle zeigen sehr subtile Indikatoren für DANE erfolgreich ausgehandelte Nachrichten.

Die letzte ausgehende TLS-Aushandlung enthält eine leicht geänderte Ausgabe, die die Domäne am Ende des Protokolleintrags enthält.

Der Protokolleintrag enthält "TLS Success Protocol", gefolgt von TLS-Version/Verschlüsselung "für domain.com".

Der Zauber liegt im "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
```

Debugging von Mail-Protokollen

Benutzerdefinierte Mail-Protokolle auf Debug-Ebene zeigen vollständige DANE- und dnssec-Suchvorgänge, erwartete Aushandlung, Teile der Überprüfung, welche erfolgreich/fehlgeschlagen sind, und einen Erfolgsindikator an.

> **Hinweis: Mail-Protokolle, die für die Protokollierung auf Debug-Ebene konfiguriert sind, können in Abhängigkeit von Systemauslastung und Konfiguration übermäßige Ressourcen auf einer ESA beanspruchen.**

Mail-Protokolle, die für die Protokollierung auf Debug-Ebene konfiguriert sind, können in Abhängigkeit von Systemauslastung und Konfiguration übermäßige Ressourcen auf einer ESA beanspruchen.

E-Mail-Protokolle werden in der Regel für längere Zeit NICHT auf Debug-Ebene verwaltet.

Die Debug Level-Protokolle können in kurzer Zeit ein enormes Volumen an E-Mail-Protokollen generieren.

Häufig wird ein zusätzliches Protokoll-Abonnement für mail_logs_d erstellt und die Protokollierung für DEBUG festgelegt.

Die Aktion verhindert Auswirkungen auf die vorhandenen mail_logs und ermöglicht die Manipulation des Volumens der Protokolle, die für das Abonnement verwaltet werden.

Um die Menge der erstellten Protokolle zu kontrollieren, beschränken Sie die Anzahl der zu pflegenden Dateien auf eine kleinere Anzahl, z. B. 2-4 Dateien.

Wenn die Überwachung, der Testzeitraum oder die Fehlerbehebung abgeschlossen sind, deaktivieren Sie das Protokoll.

Mail-Protokolle für Debug-Ebene zeigen sehr detaillierte DANE-Ausgabe an:

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)
```

Zugehörige Informationen

- ESA-Benutzerhandbücher
- Versionshinweise zum ESA
- ESA CLI-Referenzhandbücher