DANE per Email Security Appliance

Sommario

Introduzione

Questo documento descrive l'implementazione DANE per il flusso di posta in uscita ESA.

Prerequisiti

Conoscenza generale dei concetti e della configurazione ESA.

Requisiti per l'implementazione di DANE:

- Sistema di risoluzione DNS compatibile con DNSSEC
- ESA con AsyncOS 12.0 o versione successiva

Premesse

Il DANE è stato introdotto nel SEC 12 per la convalida della posta in uscita.

Autenticazione basata su DNS di entità denominate (DANE).

- DANE è un protocollo di sicurezza Internet che consente di associare certificati digitali X.509 a nomi di dominio tramite DNSSEC. (RFC 6698)
- DNSSEC è un insieme di specifiche IETF per la protezione dei record DNS tramite l'utilizzo della crittografia a chiave pubblica. (Spiegazione molto elementare. RFC 4033, RFC 4034 e RFC 4035)

Considerazioni per l'implementazione

Verificare che l'ESA utilizzi un sistema di risoluzione DNS compatibile con dnssec.

Per implementare DANE è necessaria la funzionalità DNS per eseguire query dnssec/DANE.

Per testare la funzionalità DANE DNS dell'ESA è possibile eseguire un semplice test dal login CLI dell'ESA.

Il comando CLI 'daneverify' eseguirà le query complesse per verificare se un dominio è in grado di passare la verifica DANE.

Lo stesso comando può essere utilizzato con un dominio sicuramente funzionante per confermare la capacità dell'ESA di risolvere le query dnssec.

'ietf.org' è un'origine nota a livello globale. L'esecuzione del comando cli 'daneverify' consente di verificare se il sistema di risoluzione DNS supporta o meno DANE.

PASSAGGIO VALIDO: RISULTATI "DANE SUCCESS" DEL SERVER DNS COMPATIBILE CON DANE PER 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.
```

ERRORE NON VALIDO: RISULTATI "FALSI" DEL SERVER DNS NON DANE PER ietf.org

```
> daneverify ietf.org

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

ERRORE VALIDO: daneverify cisco.com > cisco non ha implementato DANE. Questo è il risultato previsto da un resolver che supporta 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.
```

Se le prove di cui sopra funzionano in modo "VALIDO":

- Un approccio prudente consiste nel testare ogni dominio prima di aggiungere un profilo per il dominio.
- Un approccio più aggressivo sarebbe quello di configurare DANE sul profilo dei controlli di destinazione di default e vedere chi supera/non supera i controlli.

Direzione posta determina se DANE eseguirà la verifica.

I criteri di flusso del gruppo di mittenti/posta con l'azione "INOLTRA" configurata eseguiranno la verifica DANE.

I criteri di flusso del gruppo di mittenti/posta per i quali è configurata l'azione "ACCETTO" NON eseguiranno la verifica DANE.

> **Attenzione:** Se l'ESA ha abilitato i controlli di destinazione "DANE" sulla **politica predefinita**, **vi è il rischio di mancata consegna.** Se un dominio di proprietà interna, ad esempio quelli elencati nell'RAT, passa attraverso i criteri di flusso di posta RELAY e ACCEPT, insieme alla presenza di una route SMTP per il dominio.

Route SMTP

DANE non riuscirà sulle route SMTP a meno che "Host di destinazione" non sia configurato su "USEDNS".

DANE Opportunistic non recapita i messaggi che li contengono nella coda di recapito fino alla scadenza del timer del profilo di rimbalzo.

Perché? La verifica DANE viene ignorata perché una route SMTP rappresenterebbe una modifica della destinazione effettiva e potrebbe non utilizzare correttamente il DNS.

Soluzione: Creare profili di controllo destinazione per disabilitare in modo esplicito la verifica DANE per i domini contenenti route SMTP

DANE Opportunistico o DANE Obbligatorio

Le seguenti ricerche vengono eseguite durante la verifica DANE.

Ogni verifica alimenta il contenuto per eseguire la verifica successiva.

- La ricerca dei record MX verifica se >>> è sicura, non sicura e falsa
- Una ricerca di record verifica se >>> Sicuro non sicuro > Falso
- La ricerca dei record TLSA verifica se >>> Secure, Insecure, Bogus, NXDOMAIN
- Verifica certificato >> Riuscita, non riuscita

Sicurezza:

- Il DNS ha verificato la presenza di un record sicuro contenente un DS RRSIG convalidato e firmato e DNSKEY, in tutta la catena di attendibilità.

Non sicuro:

- Il DNS determina che nel dominio non sono presenti record abilitati per dnssec.

Falso:

- Incompleto, ma la verifica delle voci dnssec correnti potrebbe non riuscire.
- Record non validi a causa di una chiave scaduta.
- Record o chiave mancante nella catena di attendibilità.

NXDOMAIN

- Nessun record trovato nel DNS.

Una combinazione del controllo dei record di cui sopra e dei risultati della verifica determinerà il successo di DANE | Errore DANE | DANE fallback su TLS."

Esempio: se non viene inviato alcun RRSIG per il record MX di example.com, la zona padre (.com) viene controllata per verificare se example.com ha un record DNSKEY, indicando che example.com deve firmare i propri record. Questa convalida prosegue lungo la catena di attendibilità fino a raggiungere la verifica della chiave della zona radice (.) e le chiavi della zona radice corrispondono a quanto previsto dall'ESA (valori hardcoded sull'ESA, che viene aggiornato automaticamente in base a RFC5011).

DANE OBBLIGATORIO

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 OBBLIGATORIO

Nota: DANE OPPORTUNISTIC **NON SI COMPORTA COME TLS PREFERITO**. La parte ACTION del grafico riportato di seguito restituisce DANE FAIL, che non viene consegnato

per Obbligatorio o Opportunistico. I messaggi rimarranno nella coda di recapito fino alla scadenza del timer, quindi il recapito terminerà.

DANE OPPORTUNISTA

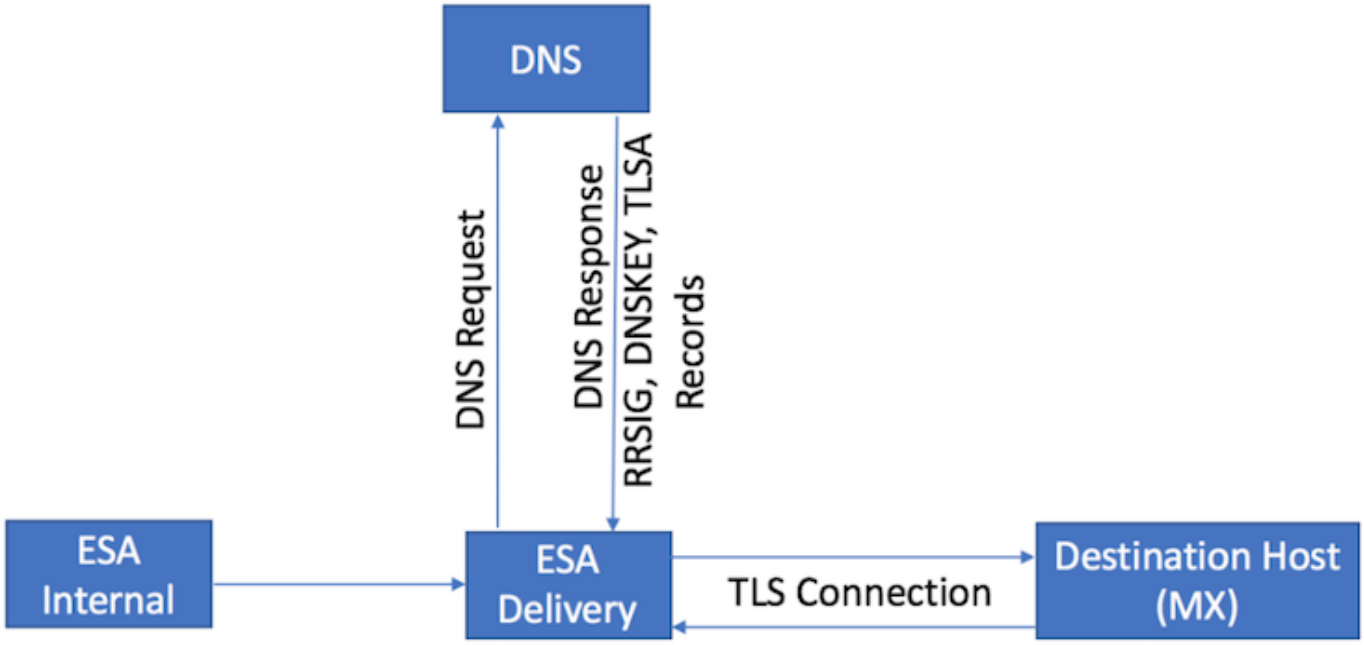
MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed →	DANE Fail
Secure	Secure	Insecure		Fallback to opportunistic TLS flow
Secure	secure	NXDOMAIN		Fallback to opportunisticTLS flow
Secure	Secure	Bogus	→	DANE Fail
Secure	Insecure	Mail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

Abilitare DANE in ambienti con più appliance

Nella figura seguente viene illustrato il flusso di lavoro quando si attiva DANE in un ambiente con più accessori.

Se nell'ambiente sono presenti più livelli di appliance ESA, uno per la scansione e l'altro per la trasmissione dei messaggi. Assicurarsi che DANE venga configurato solo sull'appliance che si connette direttamente alle destinazioni esterne.



Design Multi-ESA. DANE configurato sull'ESA di consegna

Gestione di più resolver DNS

Se per un'ESA sono configurati più resolver DNS, alcuni che supportano DNSSEC altri che non supportano DNSSEC, Cisco consiglia di configurare i resolver compatibili con DNSSEC con una priorità più alta (valore numerico inferiore), per evitare incoerenze.

In questo modo il resolver non DNSSEC non è in grado di classificare il dominio di destinazione che supporta DANE come 'Bogus'.

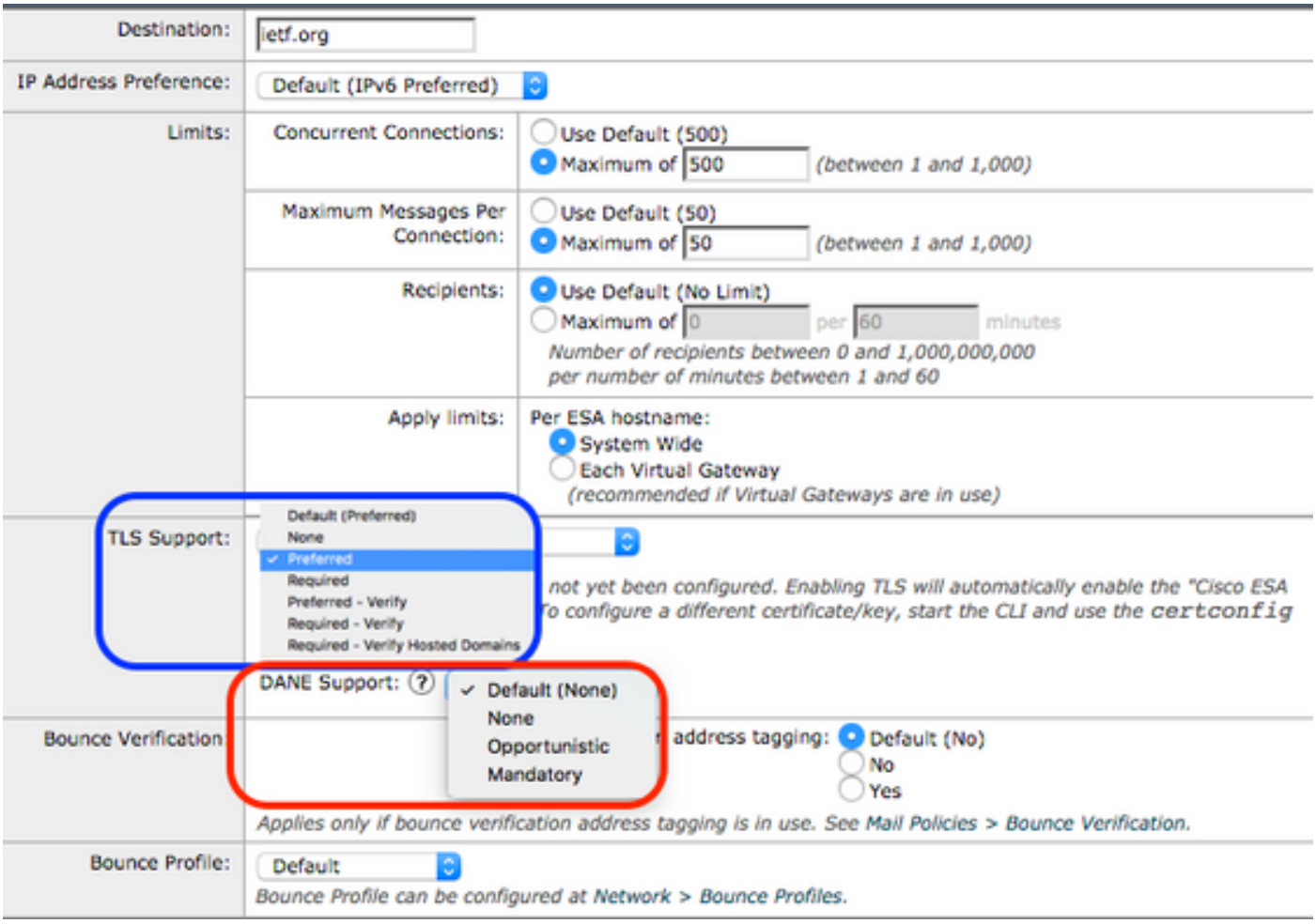
Gestione del server DNS secondario

Quando il resolver DNS non è raggiungibile, il DNS torna al server DNS secondario. Se non si configura DNSSEC sul server DNS secondario, i record MX per i domini di destinazione compatibili con DANE vengono classificati come "Bogus". Ciò influisce sul recapito del messaggio indipendentemente dalle impostazioni DANE (Opportunistica o Obbligatoria). Cisco consiglia di utilizzare un sistema di risoluzione DNSSEC secondario.

Configurazione

Configurare DANE per il flusso di posta in uscita.

1. Webui Selezionare > Mail Policies > Destination Controls > Add Destination
2. Completare la parte superiore del profilo in base alle proprie preferenze.
3. Supporto TLS: **deve essere impostato su "TLS Preferred | Preferito - Verifica | Obbligatorio | Obbligatorio - Verifica| Obbligatorio - Verifica dominio ospitato**."
4. Dopo aver abilitato il supporto TLS, il supporto DANE: il menu a discesa diventa attivo.
5. **Supporto DANE: le opzioni includono "Nessuno | Opportunistico | Obbligatorio.**
6. Una volta completata l'opzione di supporto DANE, inviare e confermare le modifiche.



Profilo di controllo destinazione - Verifica DANE

Verifica riuscita DANE

Stato consegna

Monitorare il report WebUI sullo stato di recapito per individuare eventuali creazioni non intenzionali dei domini di destinazione, potenzialmente dovute a errori DANE.

Eseguire questa operazione prima di attivare il servizio, quindi periodicamente per diversi giorni per garantire il successo continuo.

ESA WebUI > Monitor > Stato consegna > controllare la colonna "Destinatari attivi".

Log di posta

Log di posta predefiniti a livello informativo per il log.

I log di posta mostrano indicatori molto sottili per i messaggi DANE negoziati correttamente.

La negoziazione TLS finale in uscita includerà un output leggermente modificato in modo da includere il dominio alla fine della voce del log.

La voce registrata nel log include "TLS success protocol" seguito da TLS version/cipher "for domain.com".

La magia sta nel "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
```

Debug dei log di posta

I log di posta personalizzati a livello di debug visualizzano le ricerche DANE e dnssec complete, le negoziazioni previste, le parti del controllo superate/non riuscite e un indicatore di riuscita.

> **Nota: I log di posta configurati per la registrazione a livello di debug possono consumare risorse eccessive su un'ESA a seconda del carico del sistema e della configurazione.**

I log di posta configurati per la registrazione a livello di debug possono consumare risorse eccessive su un'ESA a seconda del carico del sistema e della configurazione.

I log di posta in genere NON vengono gestiti a livello di debug per lunghi periodi di tempo.

I registri a livello di debug possono generare un enorme volume di log di posta in un breve periodo di tempo.

Una procedura frequente consiste nel creare una sottoscrizione di log aggiuntiva per mail_logs_d e impostare la registrazione per DEBUG.

L'azione impedisce l'impatto sui mail_logs esistenti e consente la modifica del volume dei log gestiti per la sottoscrizione.

Per controllare il volume dei log creati, limitare il numero di file da mantenere a un numero inferiore, ad esempio 2-4 file.

Al termine del monitoraggio, del periodo di prova o della risoluzione dei problemi, disabilitare il registro.

I log di posta impostati per il livello di debug mostrano un output DANE molto dettagliato:

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)
```

Informazioni correlate

- Guide per l'utente ESA
- Note release ESA
- Guide di riferimento CLI ESA