DANE para dispositivo de seguridad de correo electrónico

Contenido

Introducción

Este documento describe la implementación de DANE para el flujo de correo saliente ESA.

prerrequisitos

Conocimiento general de los conceptos y la configuración de ESA.

Requisitos para implementar DANE:

- Resolver DNS con capacidad DNSSEC
- ESA con AsyncOS 12.0 o posterior

Antecedentes

DANE se ha introducido en el ESA 12 para la validación de correo saliente.

Autenticación basada en DNS de entidades con nombre (DANE).

- DANE es un protocolo de seguridad de Internet que permite que los certificados digitales X.509 se enlacen a nombres de dominio mediante DNSSEC. (RFC 6698)
- DNSSEC es una colección de especificaciones IETF para proteger los registros DNS

mediante el uso de criptografía de clave pública. (Explicación muy elemental. RFC 4033, RFC 4034 y RFC 4035)

Consideraciones para la implementación

Verifique que el ESA utilice un DNS Resolver compatible con dnssec.

Para implementar DANE, se requiere la capacidad DNS para realizar consultas dnssec/DANE.

Para probar la función ESA DNS DANE se puede realizar una prueba sencilla desde el inicio de sesión ESA CLI.

El comando CLI 'daneverify' realizará las consultas complejas para verificar si un dominio es capaz de pasar la verificación DANE.

El mismo comando se puede utilizar con un buen dominio conocido para confirmar la capacidad ESA para resolver consultas dnssec.

'ietf.org' es una fuente mundialmente conocida. Al ejecutar el comando cli 'daneverify', se verificará si el Resolver DNS es compatible con DANE o no.

PASO VÁLIDO: RESULTADOS "DANE SUCCESS" DEL SERVIDOR DNS CAPABLE PARA DANE PARA 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.
```

FALLO NO VÁLIDO: RESULTADOS "BOGUS" DEL SERVIDOR DNS NO DANE PARA ietf.org

```
> daneverify ietf.org

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

FALLO VÁLIDO: daneverify cisco.com > cisco no ha implementado DANE. Éste es el resultado esperado de un resoltor con capacidad 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 las pruebas "VÁLIDAS" anteriores funcionan:

- Un enfoque prudente sería probar cada dominio antes de agregar un perfil para el dominio.
- Un enfoque más agresivo sería configurar DANE en el perfil de controles de destino predeterminados y ver quién pasa/falla.

Mail Direction determina si DANE verificará.

Las políticas de flujo de correo/grupo de remitentes que tienen configurada la acción "RELAY" realizarán la verificación DANE.

Las políticas de flujo de correo/grupo de remitentes que tienen configurada la acción "ACCEPT" NO realizarán la verificación de DANE.

> **Precaución:** Si el ESA tiene los controles de diseño "DANE" habilitados en la **Política predeterminada**, **existe el riesgo de que se produzca un error en la entrega.** Si un dominio de propiedad interna como los enumerados en la RAT, pase por las políticas de flujo de correo RELAY y ACCEPT, combinadas con la presencia de una ruta SMTP para el dominio.

Rutas SMTP

DANE fallará en las rutas SMTP a menos que el "Host de Destino" esté configurado como "USEDNS".

DANE Opportunistic no entregará los mensajes, los contendrá en la cola de entrega hasta que venza el temporizador del perfil de rebote.

¿Por qué? Se omite la verificación de DANE, ya que una ruta SMTP sería una modificación del destino verdadero y puede que no utilice correctamente DNS.

Solución: Crear perfiles de control de destino para deshabilitar explícitamente la verificación DANE para dominios que contienen rutas SMTP

DANE Oportunistic o DANE Obligatorio

Las siguientes búsquedas se realizan durante la verificación de DANE.

Cada verificación alimenta el contenido para realizar la verificación posterior.

- La búsqueda de registros MX verifica si >> Secure, Insecure, Bogus
- Una búsqueda de registros verifica si >> Secure Insecure > Bogus

- La búsqueda de registros TLSA verifica si >>> Seguro, Inseguro, Falso, NXDOMAIN
- Certificado verificado >> Correcto, Fallo

Seguro:

- DNS verificó la presencia de un registro seguro que contiene un RRSIG firmado RRSIG DS y DNSKEY validados, en la cadena de confianza.

Inseguro:

- DNS determina que el dominio no tiene registros dnssec habilitados presentes.

Falso:

- Incompleto, pero las entradas dnssec presentes pueden fallar en la verificación.
- Registros no válidos debido a una clave vencida.
- Falta el registro o la clave en la cadena de confianza.

NXDOMAIN

- No se ha encontrado ningún registro en DNS.

Una combinación de la comprobación de registro anterior y los resultados de la verificación determinará "DANE Success | DANE Fail | DANE fallback to TLS."

Por ejemplo: si no se envía ningún RRSIG para el registro MX de example.com, se comprueba la zona primaria (.com) para ver si example.com tiene un registro DNSKEY, lo que indica que example.com debería estar firmando sus registros. Esta validación continúa en la cadena de confianza terminando con la verificación de clave de la zona raíz (.) y las claves de la zona raíz coinciden con lo que espera el ESA (valores codificados en el ESA, que se actualizan automáticamente según 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

Nota: DANE OPPORTUNISTIC **NO SE COMPORTA COMO TLS PREFERIDO**. La parte ACCIÓN del siguiente gráfico da como resultado DANE FAIL, no se realizará para Obligatorio ni Oportunista. Los mensajes permanecerán en la cola de entrega hasta que caduque el temporizador y, a continuación, la entrega finaliza.

DANE OPPORTUNISTIC

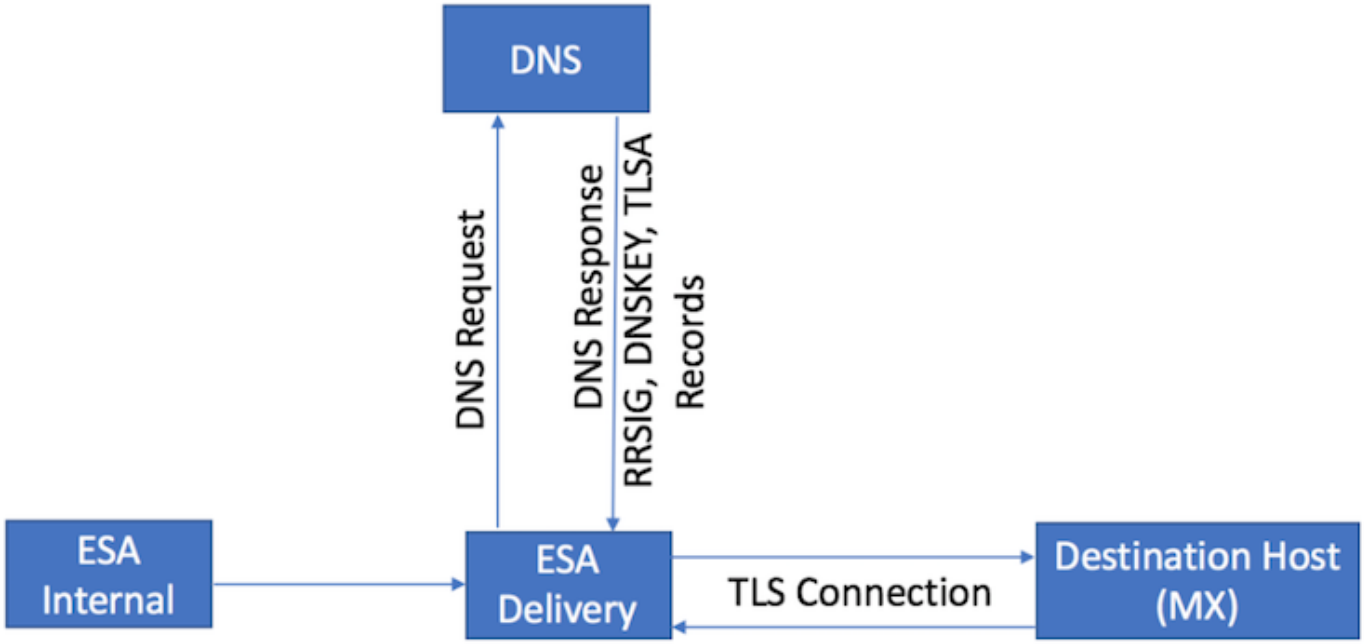
MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed →	DANE Fail
Secure	Secure	Insecure		Fallback to opportunistic TLS flow
Secure	secure	NXDOMAIN		Fallback to opportunisticTLS flow
Secure	Secure	Bogus	→	DANE Fail
Secure	Insecure	Mail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

Habilitar DANE en entornos de varios dispositivos

La siguiente figura ilustra el flujo de trabajo cuando se habilita DANE en un entorno de dispositivo múltiple.

Si el entorno tiene varias capas de dispositivos ESA, una para el escaneo y otra para el envío de mensajes Asegúrese de que DANE sólo se configure en el dispositivo que se conecta directamente a los destinos externos.



Diseño Multi-ESA. DANE configurado en el ESA de entrega

Administración de Varios Resueltos DNS

Si un ESA tiene varios resolvers DNS configurados, unos pocos que admiten DNSSEC unos pocos que no admiten DNSSEC, Cisco recomienda configurar los resolvers con capacidad DNSSEC con una prioridad más alta (valor numérico inferior), para evitar inconsistencias.

Esto evita que el solucionador no compatible con DNSSEC clasifique el dominio de destino que admite DANE como 'falso'.

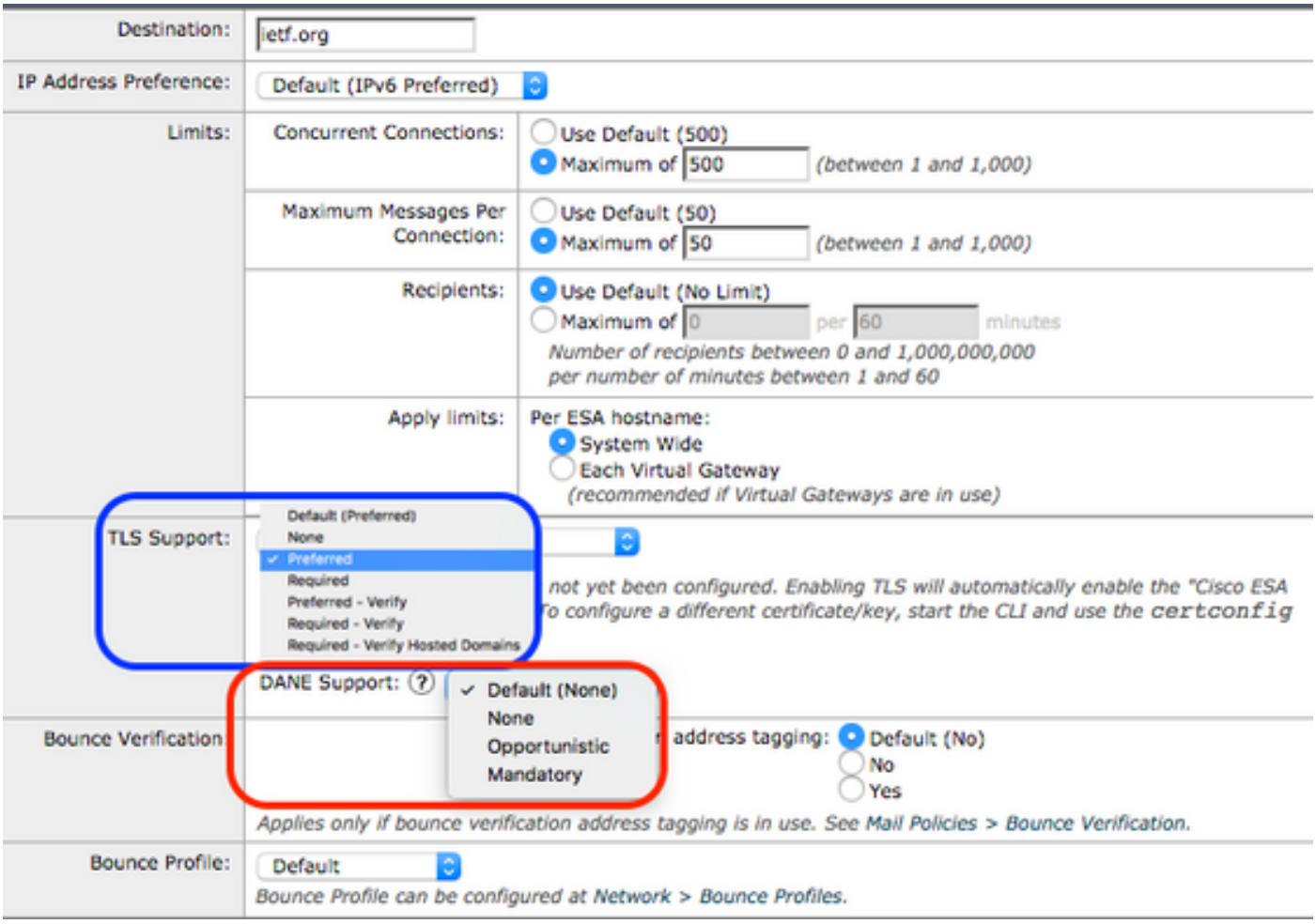
Administración del servidor DNS secundario

Cuando no se puede alcanzar la resolución de DNS, el DNS vuelve al servidor DNS secundario. Si no configura DNSSEC en el servidor DNS secundario, los registros MX para los dominios de destino compatibles con DANE se clasifican como "falsos". Esto afecta a la entrega de mensajes independientemente de la configuración de DANE (Oportunista o Obligatoria). Cisco recomienda utilizar un solucionador secundario con capacidad DNSSEC.

Configuración

Configure DANE para el flujo de correo saliente.

1. Web Vaya a > Políticas de correo > Controles de destino > Agregar destino
2. Complete la parte superior del perfil según sus preferencias.
3. Soporte de TLS: **se requiere establecer en "TLS preferido | Preferido - Verificar | Obligatorio | Requerido - Verificar| Requerido - Verificar Dominio Alojado**".
4. Una vez que se ha habilitado el soporte de TLS, DANE Support (Soporte de DANE): el menú desplegable se activará.
5. **Soporte de DANE: opciones incluyen "Ninguno" | Oportunista | Obligatorio.**
6. Una vez completada la opción DANE Support (Asistencia de DANE), envíe y confirme los cambios.



Perfil de control de destino - Verificación de DANE

Verificar el éxito de DANE

Estado de entrega

Supervise el informe "Estado de entrega" de WebUI para cualquier acumulación no intencionada de dominios de destino, posiblemente debido a una falla de DANE.

Realice esto antes de activar el servicio y, a continuación, de forma periódica durante varios días para garantizar un éxito continuo.

ESA WebUI > Monitor > Delivery Status > marque la columna "Destinatarios activos".

Registros de correo

Registros de correo predeterminados a nivel informativo para el nivel de registro.

Los registros de correo muestran indicadores muy sutiles para los mensajes negociados con éxito DANE.

El resultado final de la negociación TLS saliente incluirá una salida ligeramente modificada para incluir el dominio al final de la entrada de registro.

La entrada del registro incluirá "protocolo de éxito de TLS" seguido de la versión/cifra de TLS "para dominio.com".

La magia está en el "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
```

depuración de registros de correo

Los registros de correo personalizados en el nivel de depuración mostrarán las búsquedas DANE y dnssec completas, las negociaciones esperadas, las partes de la verificación que pasan/fallan y un indicador de éxito.

> **Nota: Los registros de correo configurados para el registro del nivel de depuración pueden consumir recursos excesivos en un ESA, dependiendo de la carga y configuración del sistema.**

Los registros de correo configurados para el registro del nivel de depuración pueden consumir recursos excesivos en un ESA, dependiendo de la carga y configuración del sistema.

Los registros de correo generalmente NO se mantienen en el nivel de depuración durante periodos prolongados.

Los registros de nivel de depuración pueden generar un enorme volumen de registros de correo en un corto período de tiempo.

Una práctica frecuente es crear una suscripción de registro adicional para mail_logs_d y establecer el registro para DEBUG.

La acción evita el impacto en los registros_de_correo existentes y permite la manipulación del volumen de registros que se mantienen para la suscripción.

Para controlar el volumen de registros creados, restrinja el número de archivos que se deben mantener a un número menor, como 2-4 archivos.

Cuando la supervisión, el periodo de prueba o la resolución de problemas hayan finalizado, inhabilite el registro.

Los registros de correo configurados para el nivel de depuración muestran un resultado DANE muy detallado:

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)
```

Información Relacionada

- Guías de usuario ESA
- Notas de la versión de ESA
- Guías de referencia de la CLI de ESA