DANE para dispositivo de segurança de e-mail

Contents

[Introduction](#)
[Prerequisites](#)
[Informações de Apoio](#)
[Considerações para implementação](#)
[Verifique se o ESA utiliza um DNS Resolver compatível com dnssec.](#)
[A direção do correio determina se o DANE verificará.](#)
[Rotas SMTP](#)
[DANE Oportunistic ou DANE Obrigatório](#)
[Habilitar DANE em ambientes de vários dispositivos](#)
[Gerenciamento de vários resolvedores de DNS](#)
[Gerenciamento do servidor DNS secundário](#)
[Configuração](#)
[Configure o DANE para o fluxo de correio de saída.](#)
[Perfil de controle de destino - verificação de DANE](#)
[Verifique o sucesso da DANE](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve a implementação DANE para o fluxo de correio de saída ESA.

Prerequisites

Conhecimento geral dos conceitos e da configuração do ESA.

Requisitos para implementar o DANE:

- Resolvedor DNS compatível com DNSSEC
- ESA com AsyncOS 12.0 ou mais recente

Informações de Apoio

O DANE foi introduzido no ESA 12 para validação de correio de saída.

Autenticação baseada em DNS de entidades nomeadas (DANE).

- O DANE é um protocolo de segurança da Internet que permite certificados digitais X.509, a serem vinculados a nomes de domínio usando DNSSEC. (RFC 6698)
- O DNSSEC é uma coleção de especificações IETF para proteger registros DNS através do uso de criptografia de chave pública. (Explicação muito elementar. RFC 4033, RFC 4034 e RFC 4035)

Considerações para implementação

Verifique se o ESA utiliza um DNS Resolver compatível com dnssec.

Énecessário o recurso DNS para executar consultas dnssec/DANE para implementar o DANE.

Para testar o recurso DANE DNS do ESA, um teste simples pode ser realizado a partir do login CLI do ESA.

O comando CLI 'daneverify' executará consultas complexas para verificar se um domínio é capaz de passar na verificação de DANE.

O mesmo comando pode ser usado com um domínio em boas condições para confirmar a capacidade do ESA para resolver consultas dnssec.

'ietf.org' é uma fonte mundialmente conhecida. A execução do comando cli 'daneverify' verificará se o DNS Resolver é compatível ou não com DANE.

PASSO VÁLIDO: RESULTADOS DE "SUCESSO DE DANE" DO SERVIDOR DNS CAPAZ DE 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.
```

FALHA INVÁLIDA: RESULTADOS "BOGUS" DO SERVIDOR DNS NÃO-DANE PARA ietf.org

```
> daneverify ietf.org

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

FALHA VÁLIDA: daneverify cisco.com > cisco não implementou DANE. Este é o resultado esperado de um resolvedor com capacidade para 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 o teste acima funcionar como "VÁLIDO":

- Uma abordagem cautelosa seria testar cada domínio antes de adicionar um perfil para o domínio.
- Uma abordagem mais agressiva seria configurar o DANE no perfil de controles de destino padrão e ver quem passa/falha.

A direção do correio determina se o DANE verificará.

As políticas de grupo de remetente/fluxo de e-mail com a ação "RELAY" configurada executarão a verificação de DANE.

As políticas de grupo de remetente/fluxo de e-mail que têm a ação "ACEITAR" configurada NÃO exigirão a verificação de DANE.

> **Cuidado:** Se o ESA tiver os controles de destino "DANE" habilitados na **política padrão**, **há um risco de falha na entrega.** Se um domínio de propriedade interna, como os listados no RAT, passe pelas políticas de fluxo de e-mail RELAY e ACCEPT, combinadas com a presença de uma Rota SMTP para o domínio.

Rotas SMTP

O DANE falhará em rotas SMTP, a menos que o "Host de destino" esteja configurado para "USEDNS".

A DANE Opportunistic não entregará as mensagens, contendo-as na Fila de entrega até que o temporizador de perfil de devolução expire.

Por quê? A verificação de DANE é ignorada, pois uma rota SMTP seria uma modificação do destino real e pode não usar o DNS corretamente.

Solução: Criar perfis de controle de destino para desativar explicitamente a verificação de DANE para domínios que contêm rotas SMTP

DANE Oportunistic ou DANE Obrigatório

As seguintes pesquisas são realizadas durante a verificação de DANE.

Cada verificação alimenta o conteúdo para executar a verificação subsequente.

- A pesquisa do registro MX verifica se >>> é segura, insegura, falsa
- Uma pesquisa de registro verifica se >>> Seguro Inseguro > Bogus
- A pesquisa de registro TLSA verifica se >>> é segura, insegura, falsa, NXDOMAIN
- Verificação do certificado >> Êxito, Falha

Seguro:

- O DNS verificou a presença de um registro seguro contendo um RRSIG DS e DNSKEY com assinatura validada por RRSIG, na cadeia de confiança.

Inseguro:

- O DNS determina que o domínio não tem nenhum registro habilitado para dnssec presente.

Falso:

- Entradas de dnssec incompletas, mas presentes, podem falhar na verificação.
- Registros inválidos devido a uma chave expirada.
- Falta registro ou chave na cadeia de confiança.

NXDOMAIN

- Nenhum registro encontrado no DNS.

Uma combinação da verificação de registro acima com os resultados da verificação determinará o "sucesso da DANE | Falha de DANE | DANE fallback para TLS."

Por exemplo: se não houver nenhum RRSIG enviado para o registro MX de example.com, a zona pai (.com) é verificada para ver se example.com tem um registro DNSKEY, indicando que example.com deve estar assinando seus registros. Essa validação continua na cadeia de conclusão de confiança com a verificação de chave da zona raiz (.).é alcançada, e as chaves da zona raiz correspondem ao que o ESA espera (valores codificados no ESA, que é atualizado automaticamente com base no RFC5011).

DANE OBRIGATÓRIO

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 OBRIGATÓRIO

> **Nota:** DANE OPORTUNISTIC **NÃO SE COMPORTA COMO TLS PREFERIDO**. A parte AÇÃO do gráfico abaixo resulta em FALHA de DANE, não será entregue para Obrigatório

ou Oportunista. As mensagens permanecerão na fila de entrega até que o temporizador expire e a entrega termine.

DANE OPORTUNISTIC

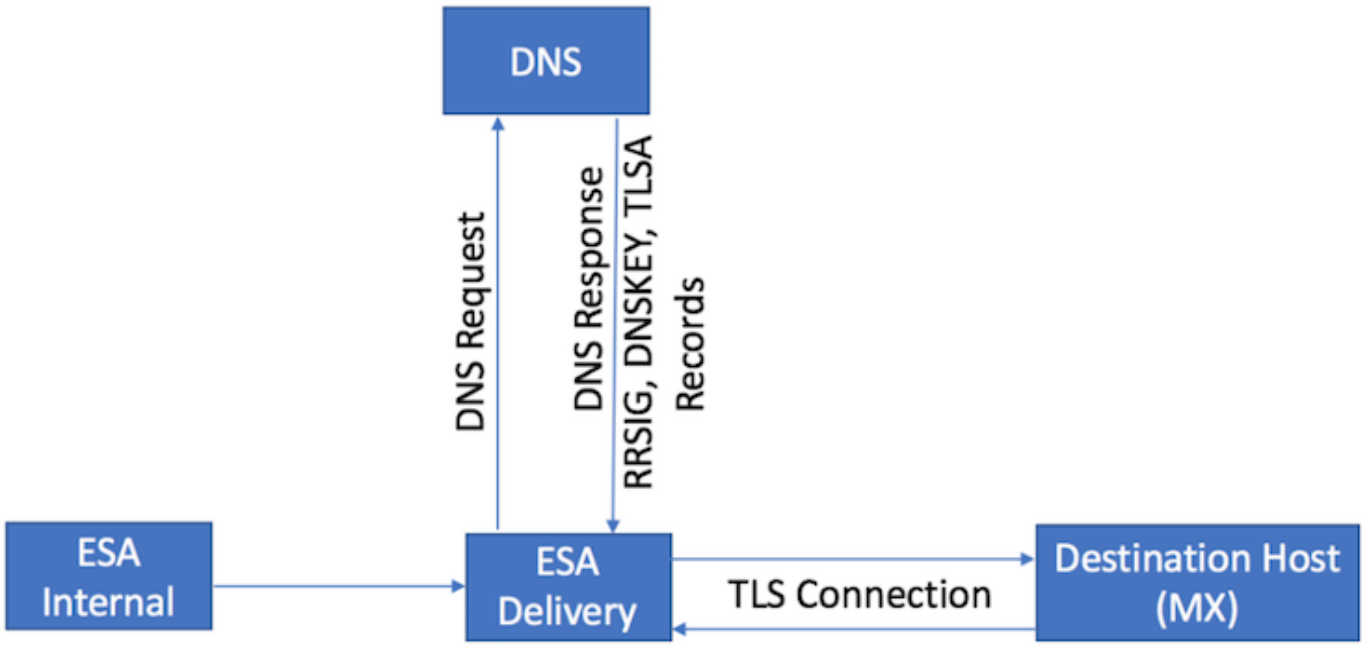
MX RECORD	A RECORD	TLSA	CERTIFICATE Verify	ACTION
Secure	Secure	Secure	Success	DANE Success
Secure	Secure	Secure	Failed →	DANE Fail
Secure	Secure	Insecure		Fallback to opportunistic TLS flow
Secure	secure	NXDOMAIN		Fallback to opportunisticTLS flow
Secure	Secure	Bogus	→	DANE Fail
Secure	Insecure	Mail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

Habilitar DANE em ambientes de vários dispositivos

A figura a seguir ilustra o fluxo de trabalho quando você habilita o DANE em um ambiente de vários dispositivos.

Se o ambiente tiver várias camadas de dispositivos ESA, uma para verificação e outra para entrega de mensagens Certifique-se de que o DANE só seja configurado no dispositivo que se conecta diretamente aos destinos externos.



Projeto Multi-ESA. DANE configurado no ESA de entrega

Gerenciamento de vários resolvedores de DNS

Se um ESA tiver vários resolvedores de DNS configurados, alguns que suportam DNSSEC alguns que não suportam DNSSEC, a Cisco recomenda configurar os resolvedores com capacidade DNSSEC com uma prioridade mais alta (valor numérico mais baixo), para evitar inconsistências.

Isso impede que o resolvedor com capacidade para Não-DNSSEC classifique o domínio de destino que suporta DANE como 'Bogus'.

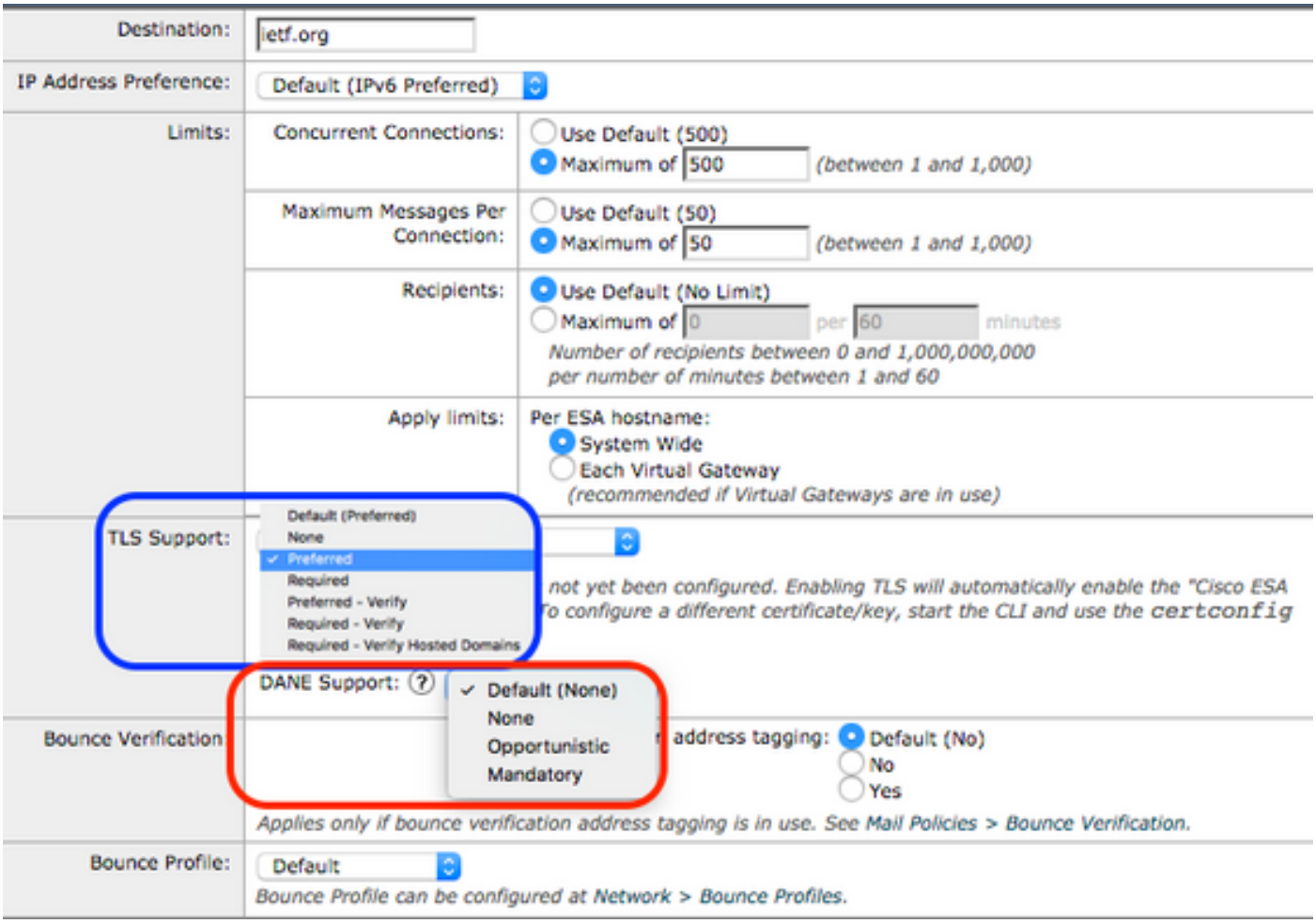
Gerenciamento do servidor DNS secundário

Quando o resolvedor DNS não pode ser alcançado, o DNS volta para o servidor DNS secundário. Se você não configurar o DNSSEC no servidor DNS secundário, os Registros MX para domínios de destino compatíveis com DANE serão classificados como "Bogus". Isso afeta a entrega da mensagem independentemente das configurações de DANE (Oportunista ou Obrigatório). A Cisco recomenda que você use um resolvedor secundário compatível com DNSSEC.

Configuração

Configure o DANE para o fluxo de correio de saída.

1. Webui Navegue até > Políticas de e-mail > Controles de destino > Adicionar destino
2. Preencha a parte superior do perfil de acordo com sua preferência.
3. Suporte TLS: **é necessário definir para "TLS preferencial | Preferencial - Verificar | Obrigatório | Obrigatório - Verificação| Obrigatória - Verificar domínio hospedado**."
4. Depois que o suporte TLS for ativado, o suporte DANE: o menu suspenso ficará ativo.
5. **Suporte DANE: as opções incluem "Nenhum | Oportunidade | Obrigatório.**
6. Depois que a opção de suporte DANE for concluída, envie e confirme as alterações.



Perfil de controle de destino - verificação de DANE

Verifique o sucesso da DANE

Status de entrega

Monitore o Relatório de "Status de Entrega" da WebUI para qualquer compilação não intencional de domínios de destino, possivelmente devido a Falha de DANE.

Faça isso antes de habilitar o serviço e depois periodicamente por vários dias para garantir o sucesso contínuo.

ESA WebUI > Monitor > Delivery Status > marque a coluna "Ative Recipients" (Destinatários ativos).

Logs de e-mail

Logs de e-mail padrão no nível informativo para o nível de log.

Os registros de e-mail mostram indicadores muito sutis para mensagens negociadas com êxito pelo DANE.

A saída final da negociação TLS incluirá uma saída ligeiramente modificada para incluir o domínio no final da entrada de log.

A entrada de registro incluirá "TLS Success Protocol" seguido de TLS version/cipher "for

domain.com".

A magia está no "para":

```
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
```

Depuração de logs de e-mail

Logs de e-mail personalizados no nível de depuração exibirão pesquisas DANE e dnssec completas, negociação esperada, partes da verificação que passam/falham e um indicador de sucesso.

> **Nota: Os logs de e-mail configurados para o log de nível de depuração podem consumir recursos excessivos em um ESA, dependendo da carga e da configuração do sistema.**

Os logs de e-mail configurados para o log de nível de depuração podem consumir recursos excessivos em um ESA, dependendo da carga e da configuração do sistema.

Os logs de e-mail geralmente NÃO são mantidos no nível de depuração por períodos prolongados.

Os logs de nível de depuração podem gerar um volume tremendo de logs de e-mail em um curto período de tempo.

Uma prática frequente é criar uma assinatura de log adicional para mail_logs_d e definir o registro para DEBUG.

A ação evita o impacto nos mail_logs existentes e permite a manipulação do volume de logs mantidos para a assinatura.

Para controlar o volume de registros criados, restrinja o número de arquivos para manter em um número menor, como 2-4 arquivos.

Quando o monitoramento, o período de avaliação ou a solução de problemas tiverem sido concluídos, desative o registro.

Os logs de e-mail definidos para o nível de depuração mostram uma saída de DANE muito detalhada:

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)
```

Informações Relacionadas

- Guias do usuário ESA
- Notas da versão do ESA
- Guias de referência da CLI do ESA