Processo de verificação TLS para a Segurança do email de Cisco

Índice

[Introdução](#)
[Processo de verificação TLS para a Segurança do email de Cisco](#)
[EU - VALIDAÇÃO CERTIFICADA](#)
[II - VALIDAÇÃO DA IDENTIDADE DO SERVER](#)
[Background](#)
[Etapa um](#)
[Etapa dois:](#)
[Verificação ESA TLS](#)
[O TLS exigido verifica](#)
[O TLS exigido verifica - Domínio hospedado](#)
[SMTPROUTES explicitamente configurado](#)
[Exemplo](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve o processo de verificação da identidade do server do Transport Layer Security (TLS) para a ferramenta de segurança do email de Cisco (o ESA)

Processo de verificação TLS para a Segurança do email de Cisco

O processo de verificação TLS é essencialmente um processo de validação de duas fases:

MIM - VALIDAÇÃO CERTIFICADA

Isto envolve a verificação de:

- período da validade de certificado - vida do certificado
- expedidor do certificate chain
- lista de revogação, etc.…

II - VALIDAÇÃO DA IDENTIDADE DO SERVER

Este é um processo de validação da **identidade apresentada** server (contida no certificado da chave pública X.509) contra a **identidade da referência do** server.

Background

Deixe-nos manter-se com a terminologia do nome da identidade descrita no RFC 6125.

> Note: **A identidade apresentada** é um identificador apresentado por um certificado da chave pública do server X.509 que possa incluir mais identificadores apresentados de um de tipos diferentes. Em caso do serviço S TP, é contida como uma extensão do subjectAltName do tipo dNSName ou como o CN (Common Name) derivado do campo de assunto.

> Note: **A identidade da referência** é um identificador construído de um Domain Name totalmente qualificado DNS que um cliente espera uns serviços de aplicativo apresentar no certificado.

O processo de verificação é na maior parte importante para um cliente TLS, porque geralmente o cliente inicia uma sessão TLS e um cliente precisa de autenticar a comunicação. *Para conseguir isto que um cliente precisa de verificar se a identidade apresentada combina a identidade da referência.* A parte importante é compreender que a Segurança do processo de verificação TLS para a entrega de correio está baseada quase inteiramente no cliente TLS.

Etapa um

A primeira etapa na validação da identidade do server é determinar a identidade da referência pelo cliente TLS. Depende do aplicativo que lista de cliente dos identificadores TLS da referência considera para ser aceitável. Igualmente uma lista de identificadores aceitáveis da referência deve ser construída independentemente dos identificadores apresentados pelo serviço. [rfs6125#6.2.1]

A identidade da referência deve ser um Domain Name totalmente qualificado DNS e pode ser analisada gramaticalmente de toda a entrada (que for aceitável para um cliente e para considerar para ser segura). A necessidade da identidade da referência de ser um nome de host DNS a que o cliente está tentando conectar.

O Domain Name destinatário do email é a identidade da referência que é expressada diretamente pelo usuário, pela intenção para enviar em particular uma mensagem a um domínio do usuário particular e esta igualmente cumpriu uma exigência ser um FQDN a que um usuário está tentando conectar. É consistente somente em caso do servidor SMTP auto-hospedado onde o servidor SMTP é possuído e controlado pelo mesmo proprietário e pelo server não está hospedando domínios demais. Como cada necessidade do domínio de ser alistado no certificado (como um do subjectAltName: valores do dNSName). De uma perspectiva de implementação, a maioria das autoridades de certificação (CA) limita o número de valor dos Domain Name a tão baixo quanto 25 entradas (como ao AS100 alto). Isto não é aceitado em caso do ambiente hospedado, deixe-nos pensam sobre os provedores de serviços do email (ESP) onde os servidores SMTP do destino hospedam milhares e mais dos domínios. Isto apenas não escala.

A identidade explicitamente configurada da referência parece ser a resposta mas esta impõe algumas limitações, porque se exige associar manualmente uma identidade da referência ao domínio de origem para cada domínio ou *"obtenção do* destino dos *dados de um serviço da terceira do mapeamento do domínio em que um usuário humano colocou explicitamente a confiança e com qual o cliente se comunicasse sobre uma conexão ou uma associação que fornecessem a autenticação mútua e a integridade que verificam". [RFC6125#6.2.1]*

Conceptualmente, isto puder ser pensado de uma único "pergunta segura MX" na altura da configuração, com o resultado posto em esconderijo permanentemente no MTA para proteger

contra todo o acordo DNS quando no estado de corrida. [2]

Isto dá uma autenticação mais forte somente com domínios do “sócio” mas para o domínio genérico que não foi traçado isto não passa o exame e o este não é igualmente imune contra alterações de configuração no lado do domínio do destino (como o hostname ou as mudanças do endereço IP de Um ou Mais Servidores Cisco ICM NT).

Etapa dois:

A próxima etapa no processo é determinar uma identidade apresentada. A identidade apresentada é fornecida por um certificado da chave pública do server X.509, como a extensão do subjectAltName do tipo dNSName ou como o Common Name (CN) encontrou no campo de assunto. Onde é perfeitamente aceitável para o campo de assunto estar vazio, enquanto o certificado contém uma extensão do subjectAltName que inclua pelo menos uma entrada do subjectAltName.

Embora o uso do Common Name seja ainda na prática ele seja considere para ser suplicado e a recomendação atual é usar entradas do subjectAltName. O apoio para a identidade da estada do Common Name para a compatibilidade retrógrada. Em tal caso um dNSName do subjectAltName deve ser usado primeiramente e somente quando está vazio o Common Name é verificado.

> **Note**: o Common Name não é datilografado fortemente porque um Common Name pôde conter uma corda humano-amigável para o serviço, um pouco do que uma corda cujo o formulário combine aquele de um Domain Name totalmente qualificado DNS

Na extremidade quando ambo o tipo de identidades foi determinado, o cliente TLS precisa de comparar cada um de seus identificadores da referência contra os identificadores apresentados com a finalidade de encontrar um fósforo.

Verificação ESA TLS

O ESA reserva permitir o TLS e a verificação de certificado na entrega aos domínios específicos (usar o destino controla a página ou o comando CLI do **destconfig**). Quando a verificação de certificado TLS é exigida, você pode escolher uma de duas opções da verificação desde a [versão 8.0.2 de](#) AsyncOS. O resultado previsto da verificação pode variar segundo a opção configurada. Dos ajustes 6 diferentes para o TLS, o controle inferior disponível do destino lá é dois importantes que são responsáveis para a verificação de certificado:

1. **TLS exigido - Verifique**
2. **TLS exigido - Verifique domínios hospedados**.

```
CLI: destconfig

Do you want to use TLS support?

1. No

2. Preferred

3. Required
```

```
4. Preferred - Verify

5. Required - Verify

6. Required - Verify Hosted Domains

[6]>
```

Um processo de verificação TLS para a opção (4) **preferida – Verify** é idêntica (5) ao **exigido – verifique**, mas a ação tomada baseada em resultados difere como a tabela abaixo dentro apresentada. Os resultados para a opção (6) **exigida – Verifique que os domínios hospedados** são idênticos (5) ao **exigido – verifique** mas um fluxo da verificação TLS é bastante diferente.

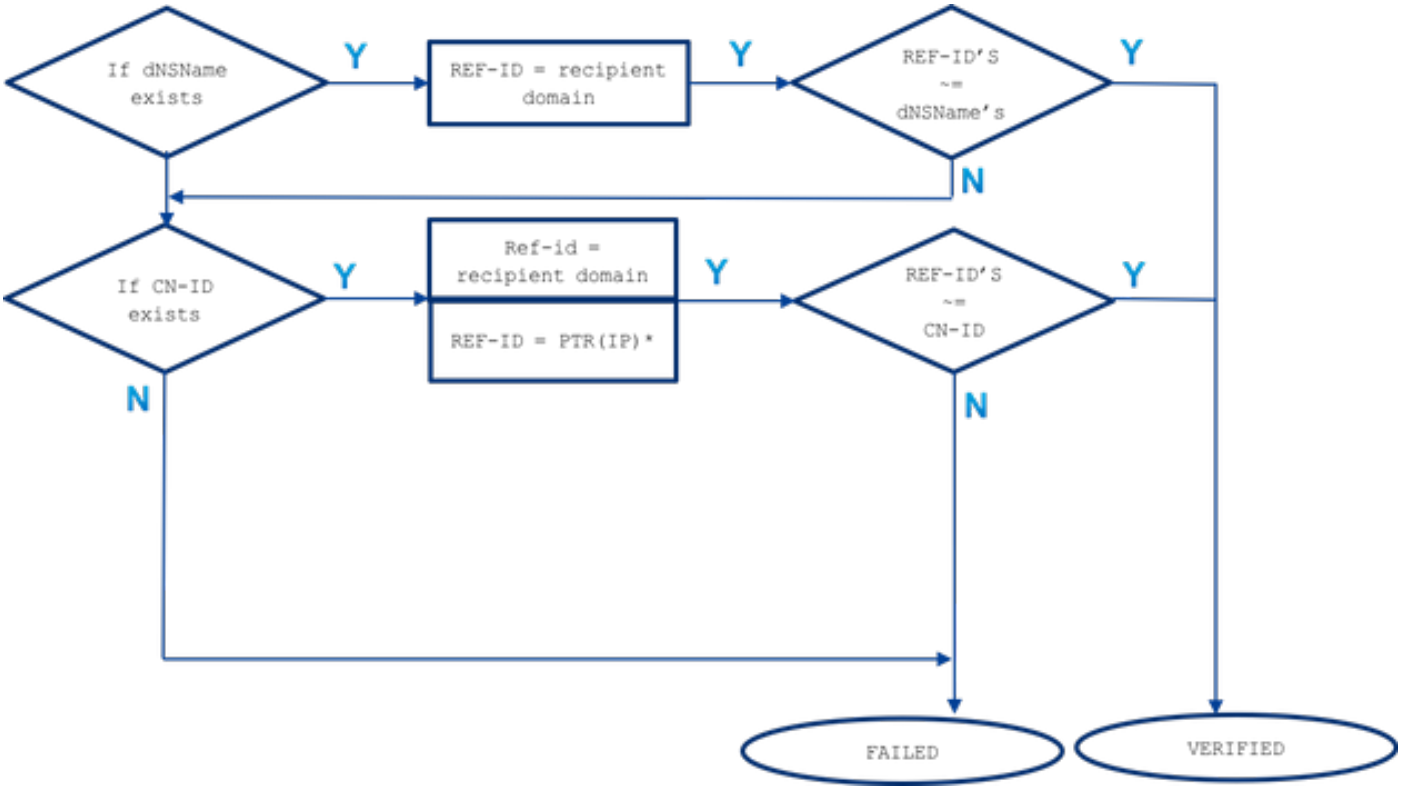
Ajustes TLS	Significado
4. Preferido (verifique)	O TLS é negociado da ferramenta de segurança do email ao MTA para o domínio. O dispositivo tenta verificar o certificado dos domínios. Três resultados são possíveis: • O TLS é negociado e o certificado é verificado. O correio é entregado através de uma sessão de criptografia. • O TLS é negociado, mas o certificado não é verificado. O correio é entregado através uma sessão de criptografia. • Nenhuma conexão TLS é feita e, o certificado não é verificado subseqüentemente. O mensagem de Email é entregado no texto simples.
5. Exigido (verifique)	O TLS é negociado da ferramenta de segurança do email ao MTA para o domínio. A verificação do certificado dos domínios é exigida. Três resultados são possíveis: • Uma conexão TLS é negociada e o certificado é verificado. O mensagem de Email é entregado através de uma sessão de criptografia. • Uma conexão TLS é negociada mas o certificado não é verificado por CA confiado. O correio não é entregado. • Uma conexão TLS não é negociada. O correio não é entregado.

A diferença entre o **TLS exigido - Verifique** e **TLS exigido - Verifique que as opções de domínio hospedadas** colocam no processo de verificação da identidade. A maneira como a identidade apresentada é processada e que tipo de identificadores da referência é permitido ser usado faz a diferença sobre um resultado final. A finalidade da descrição abaixo assim como do documento do todo é a mais próximo este processo ao utilizador final. Como a compreensão incorreta ou obscura deste assunto pode ter um impacto de Segurança na rede de usuário.

O TLS exigido verifica

A identidade apresentada é derivada primeiramente do subjectAltName - a extensão do dNSName e se há nenhuma extensão do fósforo ou do subjectAltName não existe do que CN-ID - Common Name do campo de assunto é verificada.

A lista da identidade da referência (REF-ID) é construída de um domínio destinatário ou o domínio e o hostname do receptor derivados de uma corrida da pergunta PTR DNS contra o endereço IP de Um ou Mais Servidores Cisco ICM NT o cliente são conectados a. Nota: Nesse caso particular, as identidades diferentes da referência são comparadas com as verificações apresentadas diferentes da identidade.



o ~= representa o fósforo exato ou do convite

A identidade apresentada (dNSName ou CN-ID) é comparada com as identidades aceitadas da referência até que for combinada e na ordem que estão listados abaixo.

- Se a extensão do dNSName do subjectAltName existe: o fósforo exato ou do convite é feito contra o domínio destinatário somente

  A identidade da referência em caso do fósforo do subjectAltName é derivada somente do domínio destinatário. Se o domínio destinatário não combina algumas das entradas do dNSName nenhuma identidade mais adicional da referência está verificada (como o hostname derivado da resolução de DNS MX ou PTR)

- Se o CN do assunto DN existe (CN-ID): o fósforo exato ou do convite é feito contra o domínio destinatárioo fósforo exato ou do convite é feito contra o hostname derivado da pergunta PTR executada contra um IP do servidor de destino

  Onde o registro PTR preservou uma consistência no DNS entre o remetente e o resolver. Que necessidade de ser menção aqui, esse campo do CN está comparado contra um hostname do PTR somente quando um registro PTR existir e um registro resolvido A (um remetente) para este retorno do hostname (identidade da referência) um endereço IP de Um ou Mais Servidores Cisco ICM NT que combinam um IP do servidor de destino contra que uma pergunta PTR foi executada.

  IP DO == A (PTR(IP))

  A identidade da referência em caso de CN-ID é derivada do domínio destinatário e quando não há nenhum fósforo uma pergunta DNS é executada contra um registro PTR do IP de destino para obter um hostname. Se um PTR existe uma pergunta adicional está executada

contra um registro A em um hostname derivado de um PTR para confirmar que uma consistência DNS está preservada! Nenhuma referência mais adicional é verificada (como o hostname derivado da pergunta MX)

Para resumir, com o “TLS exigido - verifique que” a opção lá não é nenhum hostname MX comparado com o dNSName ou o CN, um PTR RR DNS está verificado somente para ver se há o CN e combinado somente se consistência DNS é A preservado (PTR(IP)) = IP, exija e o teste do convite para o dNSName e o CN são executados.

O TLS exigido verifica - Domínio hospedado

A identidade apresentada é derivada primeiramente da extensão do subjectAltName do tipo dNSName. Se não há nenhuma harmonia entre o dNSName e essa das identidades aceitadas da referência (REF-ID), a verificação não falha nenhuma matéria se o CN existe no campo de assunto e poderia passar uma verificação mais adicional da identidade. O CN derivado do campo de assunto é validado somente quando o certificado não contém alguma da extensão do subjectAltName do tipo dNSName.

Recorde que a identidade apresentada (dNSName ou CN-ID) está comparada com as identidades aceitadas da referência até que for combinada e na ordem que estão listados abaixo.

- Se a extensão do dNSName do subjectAltName existe:

  Se há nenhum matchbetween o dNSName e uma de identidades aceitadas da referência alistou a validação belowthan da identidade está falhado
  o fósforo exato ou do convite é feito contra o domínio destinatário: Um do dNSName deve combinar um domínio destinatárioo fósforo exato ou do convite é feito contra explicitamente o nome de host configurado com SMTPROUTES (*)o fósforo exato ou do convite é feito contra o hostname MX derivado (um incerto) da pergunta DNS contra o Domain Name destinatário

  Se o domínio destinatário não configurou explicitamente a rota S TP com entradas FQDN e o domínio destinatário não esteve combinado do que um retorno FQDN por um MX Record (um incerto) da pergunta DNS contra um domínio destinatário é usado. Se não há nenhum fósforo nenhum teste mais adicional está executado, que nenhuns os registros PTR são verificados
- Se o CN do assunto DN existe (CN-ID):
  O CN é validado somente quando o dNSName não faz existe no certificado. O CN-ID é comparado com a lista abaixo de identidades aceitadas da referência.

  o fósforo exato ou do convite é feito contra o domínio destinatárioo fósforo exato ou do convite é feito contra explicitamente o nome de host configurado em SMTPROUTES (*)o fósforo exato ou do convite é feito contra o hostname MX derivado (um incerto) da pergunta DNS contra o Domain Name destinatário

SMTPROUTES explicitamente configurado

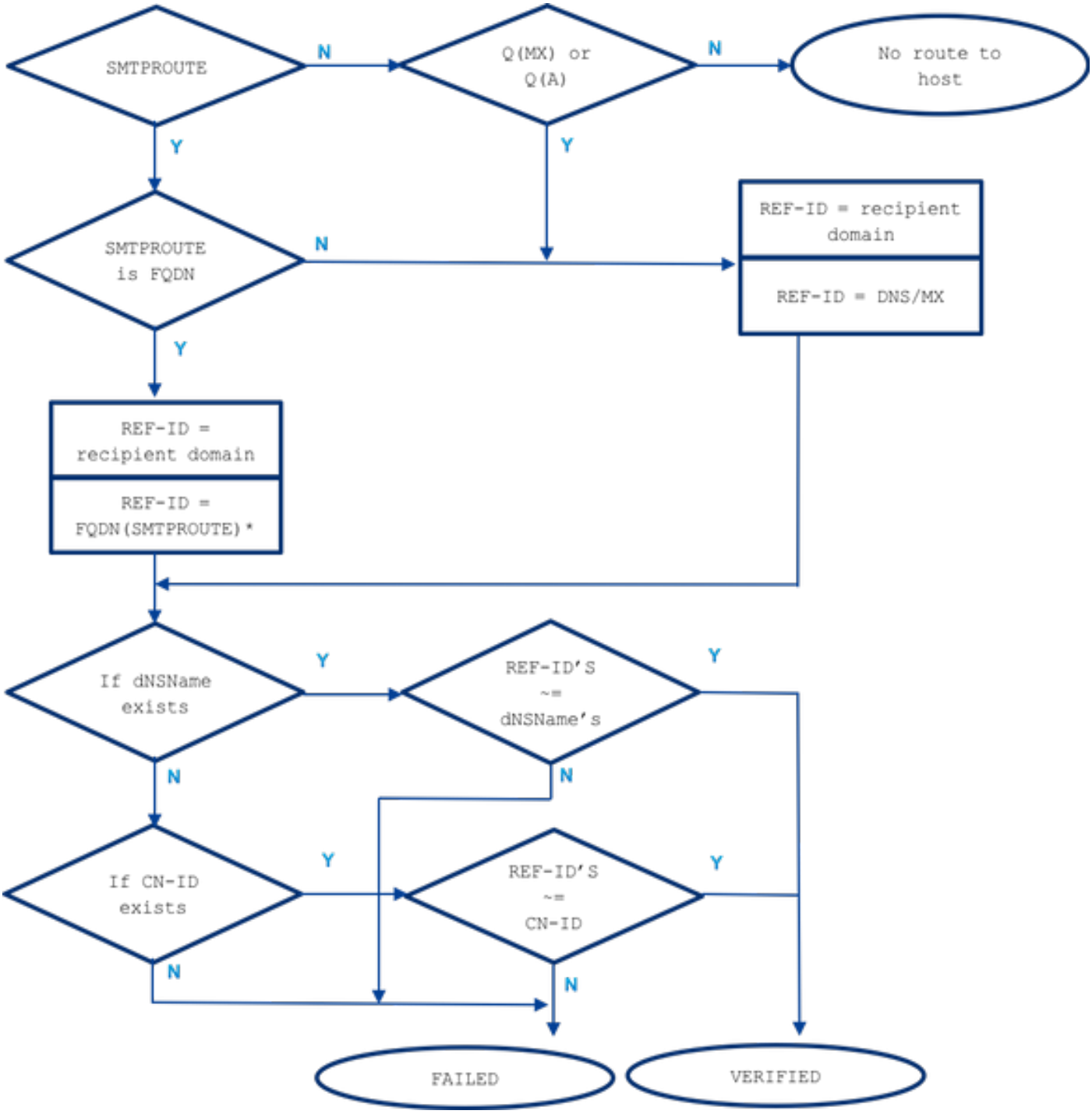
Quando a rota S TP é configurada e a identidade apresentada não combinou o domínio do receptor de e-mail então todas as rotas que FQDN os nomes são comparados e se não combinam não há nenhuma verificação mais adicional. Com o S TP explicitamente configurado não distribui nenhum hostname MX são considerados para ser comparados contra uma identidade apresentada. A exceção aqui faz uma rota S TP que seja ajustada como um endereço

IP de Um ou Mais Servidores Cisco ICM NT.

As seguintes regras aplicam-se em caso das rotas explicitamente configuradas S TP:

- Quando a rota S TP existe para um domínio destinatário e é um Domain Name totalmente qualificado DNS (FQDN) que se considera como uma identidade da referência. Este hostname (um nome da rota) é comparado com a identidade apresentada recebida de um certificado derivado de um servidor de destino a que está apontando.
- As rotas múltiplas para um domínio destinatário são permitidas. Se o domínio destinatário tem mais de uma rota S TP, as rotas estão processadas até os identificadores apresentados do certificado do servidor de destino combinarão o nome da rota a que a conexão foi estabelecida. Se os anfitriões na lista têm prioridades diferentes essas com o mais alto (0 são o mais alto e o padrão) é processado primeiramente. Se todos têm a mesma prioridade a lista de rotas está processada na ordem que as rotas foram ajustadas pelo usuário.
- Caso que quando o host não responde (não está disponível) ou responde mas a verificação TLS falhou o host seguinte da lista está processada. Quando o primeiro host está disponível e passa a verificação outro não está usado.
- Se as rotas múltiplas resolvem aos mesmos endereços IP de Um ou Mais Servidores Cisco ICM NT, simplesmente uma conexão a este IP está estabelecida e a identidade apresentada derivada do certificado enviado pelo servidor de destino deve combinar um do nome destas rotas.
- Se a rota S TP existe para domínios destinatários mas foi configurada como um endereço IP de Um ou Mais Servidores Cisco ICM NT, a rota é ainda uso fazer uma conexão mas uma identidade apresentada do certificado é comparada contra o domínio destinatário e mais adicional com o hostname derivado do registro de recurso DNS/MX.

Quando nós falamos sobre o TLS exigido verifique a opção para domínios hospedados, a maneira como o ESA conectou com um servidor de destino é importante para o processo de verificação TLS devido às rotas explicitamente configuradas S TP que fornece a identidade adicional da referência a ser considerada no processo.



o ~= representa o fósforo exato ou do convite

Exemplo

Deixe-nos tomar um exemplo da vida real, mas para o domínio destinatário: example.com. Abaixo do eu tentei descrever toda a etapa que são necessários para verificar manualmente a identidade do server.

Primeiramente, deixe-nos recolher toda a informação necessária sobre o server destinatário.

Nomes de host MX:

```
example.com -> IN MX mx01.subd.emailhosted.not.
example.com -> IN MX mx02.subd.emailhosted.not.
```

```
mx01.subd.emailhosted.not. -> IN A 192.0.2.1
mx02.subd.emailhosted.not. -> IN A 192.0.2.2
```

PTR(IP):

```
example.com -> IN MX mx01.subd.emailhosted.not.
example.com -> IN MX mx02.subd.emailhosted.not.

mx01.subd.emailhosted.not. -> IN A 192.0.2.1
mx02.subd.emailhosted.not. -> IN A 192.0.2.2
```

A (PTR(IP)):

```
example.com -> IN MX mx01.subd.emailhosted.not.
example.com -> IN MX mx02.subd.emailhosted.not.

mx01.subd.emailhosted.not. -> IN A 192.0.2.1
mx02.subd.emailhosted.not. -> IN A 192.0.2.2
```

Note: os nomes de host MX e os nomes do revDNS não combinam neste caso

Deixa agora para obter uma identidade apresentada certificado:

IDENTIDADES DOS CERTIFICADOS:

```
$ echo QUIT |openssl s_client -connect mx0a.emailhosted.not:25 -starttls smtp 2>/dev/null|
openssl x509 -text | grep -iEo 'DNS:.*|CN=.*'

CN=thawte SHA256 SSL CA
CN=*.emailhosted.not
DNS:*.emailhosted.not, DNS:emailhosted.not
```

```
echo QUIT |openssl s_client -connect mx0b.emailhosted.not:25 -starttls smtp 2>/dev/null| openssl
x509 -text | grep -iEo 'DNS:.*|CN=.*'

CN=thawte SHA256 SSL CA
CN=*.emailhosted.not
DNS:*.emailhosted.not, DNS:emailhosted.not
```

Ambos os servidores de destino têm o mesmo certificado instalado. Deixe-nos rever duas opções da validação e comparar a verificação resulta.

Em caso de usar o **TLS exigido verifique:**

A sessão TLS é estabelecida com um dos server MX e a validação da identidade começa verificando a identidade apresentada desejada:

- identidade apresentada: **o dNSName existe** (continue com comparação com a identidade permitida da referência)

  a identidade da referência = domínio destinatário (**example.com**) é verificada e **não combina o dNSName DNS: *.emailhosted.not, DNS: emailhosted.not**

- identidade apresentada: **O CN existe** (continue com o identiy em seguida apresentado quanto para ao precedente não havia nenhum fósforo)

  a identidade da referência = domínio destinatário (**example.com)** é verificada e **não combina o CN *.emailhosted.not**

  identidade da referência = PTR(IP): uma pergunta PTR é executada contra o IP do server a que o cliente TLS (ESA) tem a conexão estabelecida e recebido um certificado, e de retornos desta pergunta: **mx0a.emailhosted.not.**

  A consistência DNS é verificada para considerar este hostname como a identidade válida da referência:

```
mx01.subd.emailhosted.not. -> IN A 192.0.2.1

PTR(IP):       192.0.2.1  -> IN PTR  mx0a.emailhosted.not.
A(PTR(IP)):    mx0a.emailhosted.not. -> IN A 192.0.2.1
```

  O valor de **mx0a.emailhosted.not** é comparado contra o CN ***.emailhosted.not e** lá combina.
O Domain Name PTR valida a identidade e como o certificado é um certificado assinado de CA ele valida o certificado inteiro e a sessão TLS é estabelecida.

Em caso de usar o **TLS exigido verifique para o domínio hospedado** para este mesmo receptor:

- identidade apresentada: **o dNSName existe** (assim que o CN não será processado nesse caso) a identidade da referência = o domínio destinatário (example.com) é verificada e não combina o dNSName DNS: *.emailhosted.not, DNS: emailhosted.nota identidade da referência = o FQDN (rota smtp) - lá não são nenhum smtproutes para este domínio destinatário

  Como há nenhum SMTPROUTES usado adicionalmente:

  a identidade da referência = o MX (domínio destinatário) - uma pergunta DNS MX são executados contra o domínio destinatário
  e retornos: **mx01.subd.emailhosted.not** - isto **não combina o dNSName DNS: *.emailhosted.not, DNS: emailhosted.not**
- identidade apresentada: **O CN existe mas é saltado** enquanto o dNSName existe também.

Porque o CN não é considerado ser processado a validação da identidade TLS está falhando nesse caso assim como a verificação de certificado e em consequência conexão não pode ser estabelecida.

Informações Relacionadas

- RFC6125 - https://tools.ietf.org/html/rfc6125
- RFC2818 - https://tools.ietf.org/html/rfc2818
- AsyncOS 8.0.2 Release Note

- Suporte Técnico e Documentação - Cisco Systems