Proceso de verificación de TLS para la Seguridad del correo electrónico de Cisco

Contenido

Introducción

Este documento describe el proceso de verificación de la identidad del servidor de Transport Layer Security (TLS) para el dispositivo de seguridad del correo electrónico de Cisco (el ESA)

Proceso de verificación de TLS para la Seguridad del correo electrónico de Cisco

El proceso de verificación de TLS es esencialmente un proceso de validación de dos fases:

I - VALIDACIÓN DE CERTIFICADO

Esto implica la verificación de:

- período de la validez del certificado - curso de la vida del certificado
- emisor de la Cadena de certificados
- lista de revocación, etc….

II - VALIDACIÓN DE LA IDENTIDAD DEL SERVIDOR

Éste es un proceso de validación servidor de la **actual identidad** (contenida en el certificado de la clave pública X.509) contra la **identidad de la referencia del** servidor.

Antecedente

Guardemos con la terminología del nombre de la identidad descrita en el RFC 6125.

> Note: La actual identidad es un identificador presentado por un certificado de la clave pública del servidor X.509 que pueda incluir más de uno los actuales identificadores de diversos tipos. En caso del servicio SMTP, se contiene como extensión del subjectAltName del dNSName del tipo o como el CN (Common Name) derivado del campo Subject.

> Note: La identidad de la referencia es un identificador construido de un Domain Name calificado completamente DNS que un cliente espera que un servicio de aplicación presente en el certificado.

El proceso de verificación es sobre todo importante para un cliente de TLS, pues en general el cliente inicia una sesión de TLS y un cliente necesita autenticar la comunicación. *Para alcanzar esto que un cliente necesita verificar si la actual identidad hace juego la identidad de la referencia.* La parte importante es entender que la Seguridad del proceso de verificación de TLS para la entrega de correo está basada casi totalmente en el cliente de TLS.

Primer paso

El primer paso en la validación de la identidad del servidor es determinar la identidad de la referencia del cliente TLS. Depende de la aplicación qué lista de cliente de TLS de los identificadores de la referencia considera para ser aceptable. También una lista de identificadores aceptables de la referencia se debe construir independientemente de los identificadores presentados por el servicio. [rfs6125#6.2.1]

La identidad de la referencia debe ser un Domain Name calificado completamente DNS y se puede analizar de cualquier entrada (que sea aceptable para un cliente y considerar para ser segura). La necesidad de la identidad de la referencia de ser un nombre del host de DNS con el cual el cliente está intentando conectar.

El Domain Name receptor del correo electrónico es la identidad de la referencia que es expresada directamente por el usuario, por el intento para enviar un mensaje a un dominio del usuario determinado particularmente y ésta también cumplió un requisito de ser un FQDN con el cual un usuario está intentando conectar. Es constante solamente en caso del servidor SMTP uno mismo-recibido donde poseen al servidor SMTP y manejado por el mismo propietario y el servidor no está recibiendo demasiados dominios. Como cada necesidad del dominio de ser enumerado en el certificado (como uno de subjectAltName: valores del dNSName). Del perspectiva de implementación, la mayor parte de las autoridades de certificación limitan el número de valor de los Domain Name hasto sólo 25 entradas (hasta 100). Esto no se valida en caso del entorno alojado, déjenos piensan en los proveedores de servicio del correo electrónico (ESP) donde los servidores SMTP del destino reciben los millares y más de los dominios. Esto apenas no escala.

La identidad explícitamente configurada de la referencia parece ser la respuesta pero ésta impone algunas restricciones, pues se requiere asociar manualmente una identidad de la referencia al dominio de origen para cada dominio o la *"obtención del* destino de los *datos de un servicio de tercera persona de la asignación del dominio en el cual un usuario humano ha puesto explícitamente la confianza y con cuál comunica el cliente sobre una conexión o una asociación que proporcionen la autenticación recíproca y la integridad que marcan". [RFC6125#6.2.1]*

Conceptual, esto se puede pensar en una "interrogación segura de una sola vez MX" a la hora de la configuración, con el resultado ocultado permanentemente en el MTA para salvaguardar contra

cualquier compromiso DNS mientras que en el estado de funcionamiento. [2]

Esto da una autenticación más fuerte solamente con los dominios del “partner” pero para el dominio genérico que no se ha asociado esto no aprueba el examen y éste no es también inmune contra los cambios de configuración en el lado del dominio del destino (como el nombre de host o los cambios de la dirección IP).

“Paso dos”

El siguiente paso en el proceso es determinar una actual identidad. La actual identidad es proporcionada por un certificado de la clave pública del servidor X.509, como la extensión del subjectAltName del dNSName del tipo o como Common Name (CN) encontró en el campo Subject. Donde está perfectamente aceptable que el campo Subject esté vacío, mientras el certificado contenga una extensión del subjectAltName que incluya por lo menos una entrada del subjectAltName.

Aunque el uso del Common Name sea él siga siendo en la práctica considere para ser desaprobado y la recomendación actual es utilizar las entradas del subjectAltName. El soporte para la identidad de la estancia del Common Name para la compatibilidad descendente. En tal caso un dNSName del subjectAltName debe ser utilizado primero y solamente cuando está vacío se marca el Common Name.

> **Note**: el Common Name no se teclea fuertemente porque un Common Name pudo contener una cadena humano-cómoda para el servicio, bastante que una cadena cuya forma haga juego el de un Domain Name calificado completamente DNS

En el extremo cuando ambo han determinado al tipo de identidades, el cliente TLS necesita comparar cada uno de sus identificadores de la referencia contra los actuales identificadores con el fin de encontrar un emparejamiento.

Verificación ESA TLS

El ESA permite el habilitar de TLS y de la verificación del certificado en la salida a los dominios específicos (usando la página de los controles del destino o el comando CLI del **destconfig**). Cuando se requiere la verificación del certificado de TLS, usted puede elegir una de dos opciones de la verificación desde la versión 8.0.2 de AsyncOS. El resultado previsto de la verificación puede variar dependiendo de la opción configurada. A partir de 6 diversas configuraciones para TLS, el control inferior disponible del destino allí es dos importantes que son responsables de la verificación del certificado:

1. **TLS requirió - Verifique**
2. **TLS requirió - Verifique los dominios recibidos**.

```
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]>
```

Un proceso de verificación de TLS para la opción (4) **preferida – Verify** es idéntico (5) a **requerido – verifique**, solamente el acción realizada basado en los resultados diferencia como adentro actual tabla abajo. Los resultados para la opción (6) **requerida – Verifique los dominios recibidos** es idéntico (5) a **requerido – verifique** pero un flujo de la verificación de TLS es muy diferente.

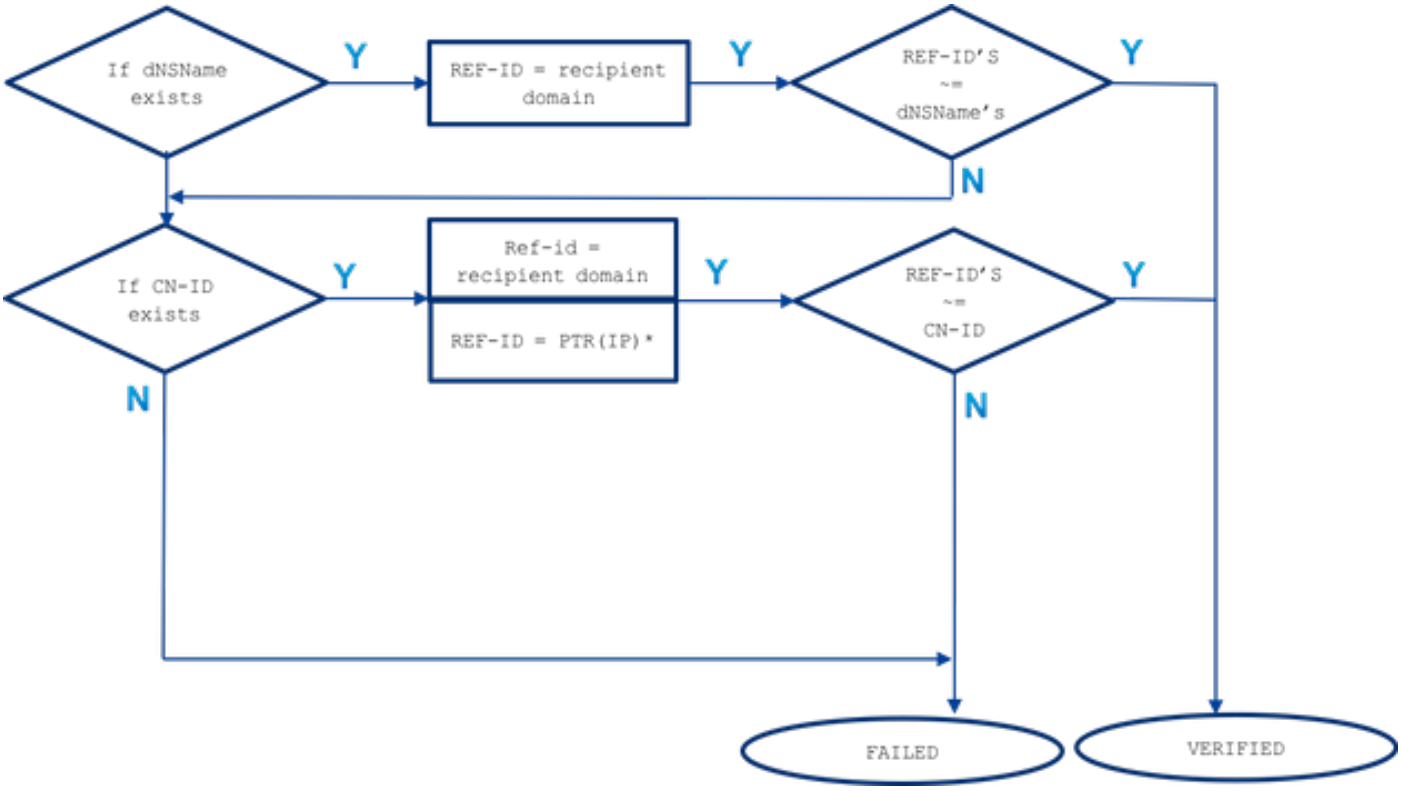
Configuraciones de TLS	Significado
4. Preferido (verifique)	TLS se negocia del dispositivo de seguridad del correo electrónico al MTA para el dominio. El dispositivo intenta verificar el certificado de los dominios. Tres resultados son posibles: • Se negocia TLS y se verifica el certificado. El correo se entrega vía una sesión encriptada. • Se negocia TLS, pero el certificado no se verifica. El correo se entrega vía una sesión encriptada. • No se hace ninguna conexión TLS y, el certificado no se verifica posteriormente. El correo electrónico se entrega en el sólo texto.
5. Requerido (verifique)	TLS se negocia del dispositivo de seguridad del correo electrónico al MTA para el dominio. La verificación del certificado de los dominios se requiere. Tres resultados son posibles: • Se negocia una conexión TLS y se verifica el certificado. El correo electrónico se entrega vía una sesión encriptada. • Se negocia una conexión TLS pero el certificado no es verificado por CA de confianza. El correo no se entrega. • Una conexión TLS no se negocia. El correo no se entrega.

La diferencia entre **TLS requirió - Verifique** y **TLS requirió - Verifique las opciones de dominio recibidas** pone en el proceso de verificación de la identidad. La manera cómo se procesa la actual identidad y se permite a qué tipo de identificadores de la referencia ser utilizado diferencia sobre un resultado final. El propósito de la descripción abajo así como del documento del conjunto es a más cercano este proceso al usuario final. Como la comprensión incorrecta o no entendible de este tema puede tener un impacto de Seguridad en la red de usuario.

TLS requirió verifica

Se marca la actual identidad se deriva primero del subjectAltName - la extensión del dNSName y si hay ninguna extensión de la coincidencia o del subjectAltName no existe que CN-ID - Common Name del campo Subject.

La lista de la identidad de la referencia (REF-ID) se construye de un dominio receptor o el dominio y el nombre de host del beneficiario derivados de un funcionamiento de la interrogación PTR DNS contra la dirección IP el cliente está conectado con. Nota: En ese caso particular, diversas identidades de la referencia se comparan con diversos actuales controles de la identidad.



el ~= representa la coincidencia exacta o del comodín

La actual identidad (dNSName o CN-ID) se compara con las identidades validadas de la referencia hasta que se corresponde con y en la orden que son mencionada abajo.

- Si existe la extensión del dNSName del subjectAltName: la coincidencia exacta o del comodín se hace contra el dominio receptor solamente

  La identidad de la referencia en caso de la coincidencia del subjectAltName se deriva solamente del dominio receptor. Si el dominio receptor no hace juego las entradas unas de los del dNSName no se marca ninguna otra identidad de la referencia (como el nombre de host derivado de la resolución de DNS MX o PTR)

- Si existe el CN del tema DN (CN-ID): la coincidencia exacta o del comodín se hace contra el dominio receptorla coincidencia exacta o del comodín se hace contra el nombre de host derivado de la interrogación PTR realizada contra un IP del servidor de destino

  Donde el expediente PTR preservó un estado coherente en el DNS entre el promotor y el software de resolución de nombres. Qué necesidad de ser mención aquí, ese campo CN se compara contra un nombre de host de la PTR solamente cuando existe un expediente PTR y un expediente resuelto A (un promotor) para esta vuelta del nombre de host (identidad de la referencia) una dirección IP que hacen juego un IP del servidor de destino contra el cual una interrogación PTR fue realizada.

  IP DEL == A (PTR(IP))

  La identidad de la referencia en caso de CN-ID se deriva del dominio receptor y cuando no hay coincidencia una interrogación DNS se realiza contra un expediente PTR del IP de destino para conseguir un nombre de host. ¡Si existe una PTR una consulta adicional se

realiza contra un expediente A en un nombre de host derivado de una PTR para confirmar que un estado coherente DNS está preservado! No se marca ninguna otra referencia (como el nombre de host derivado de la interrogación MX)

Para resumir, con “TLS requirió - verifique” la opción allí no es ningún nombre de host MX comparado con el dNSName o el CN, una PTR RR DNS se marca solamente para saber si hay CN y se corresponde con solamente si estado coherente DNS es A preservada (PTR(IP)) = IP, exija y la prueba del comodín para el dNSName y el CN se realiza.

TLS requirió verifica - Dominio recibido

La actual identidad primero se deriva de la extensión del subjectAltName del dNSName del tipo. Si no hay coincidencia entre el dNSName y el que está de las identidades validadas de la referencia (REF-ID), la verificación no falla ninguna materia si el CN existe en el campo Subject y podría pasar la verificación adicional de la identidad. El CN derivado del campo Subject se valida solamente cuando el certificado no contiene ninguna de la extensión del subjectAltName del dNSName del tipo.

Recuerde que la actual identidad (dNSName o CN-ID) está comparada con las identidades validadas de la referencia hasta que se corresponde con y en la orden que son mencionados abajo.

- Si existe la extensión del dNSName del subjectAltName:

  Si hay ningún matchbetween el dNSName y una de las identidades validadas de la referencia enumeró la validación belowthan de la identidad se falla
  la coincidencia exacta o del comodín se hace contra el dominio receptor: Uno del dNSName debe hacer juego un dominio receptorla coincidencia exacta o del comodín se hace contra explícitamente el nombre del host configurado con SMTPROUTES (*)la coincidencia exacta o del comodín se hace contra el nombre de host MX derivado (un inseguro) de la interrogación DNS contra el Domain Name receptor

  Si el dominio receptor no ha configurado explícitamente la ruta S TP con las entradas FQDN y el dominio receptor no fue correspondido con que una vuelta FQDN por un registro MX (un inseguro) de la interrogación DNS contra un dominio receptor se utiliza. Si no hay coincidencia no se realiza ningunas otras pruebas, que ningunos se marcan los expedientes PTR
- Si existe el CN del tema DN (CN-ID):
  Se valida el CN solamente cuando no lo hace el dNSName existe en el certificado. El CN-ID se compara con la lista abajo de identidades validadas de la referencia.

  la coincidencia exacta o del comodín se hace contra el dominio receptorla coincidencia exacta o del comodín se hace contra explícitamente el nombre del host configurado en SMTPROUTES (*)la coincidencia exacta o del comodín se hace contra el nombre de host MX derivado (un inseguro) de la interrogación DNS contra el Domain Name receptor

SMTPROUTES explícitamente configurado

Cuando se configura la ruta S TP y la actual identidad no hizo juego el dominio del destinatario de

correo electrónico entonces todas las rutas FQDN que se comparan los nombres y si no hacen juego no hay otros controles. Con el S TP explícitamente configurado no rutea ningún nombre de host MX se consideran para ser comparados contra una actual identidad. La excepción aquí hace una ruta S TP que fue fijada como dirección IP.

Las reglas siguientes se aplican en caso de las rutas explícitamente configuradas S TP:

- Cuando la ruta S TP existe para un dominio receptor y es un Domain Name calificado completamente DNS (FQDN) que se considera como identidad de la referencia. Este nombre de host (un nombre de la ruta) se compara con la actual identidad recibida de un certificado derivado de un servidor de destino a quien esté señalando.

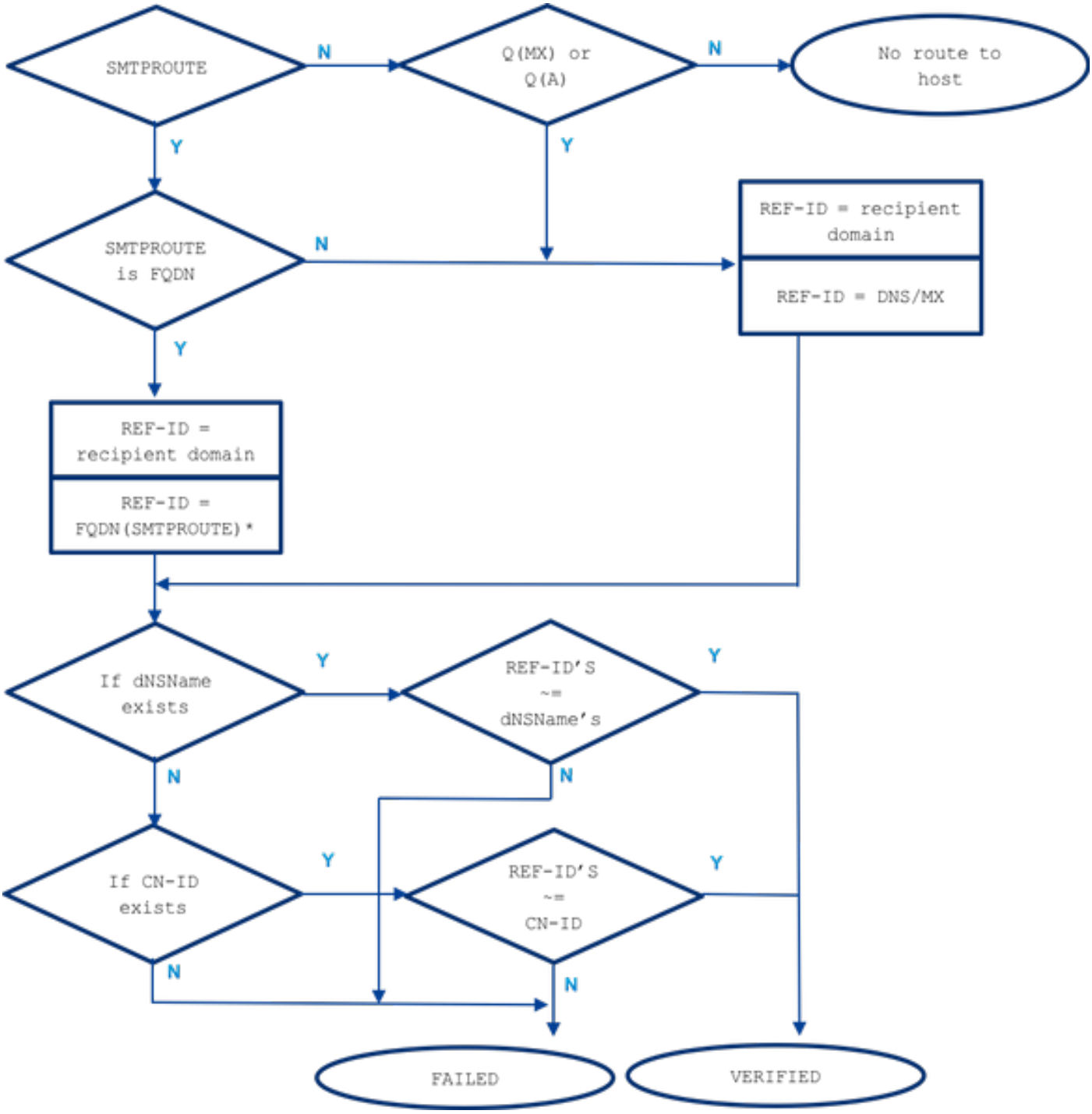
- Las rutas múltiples para un dominio receptor se permiten. Si el dominio receptor tiene más de una ruta S TP, las rutas se procesan hasta los actuales identificadores del certificado del servidor de destino harán juego el nombre de la ruta a la cual la conexión fue establecida. Si los host en la lista tienen diversas prioridades las que está con el más alto (0 es el más alto y el valor por defecto) se procesa primero. Si todos tienen la misma prioridad la lista de rutas se procesa en la orden que las rutas fueron fijadas por el usuario.

- En caso de que cuando no responde el host (no esté disponible) o responda pero se procesa la verificación de TLS ha fallado el host siguiente de la lista. Cuando el primer host está disponible y pasa la verificación otros no se utilizan.

- Si el múltiplo rutea las resoluciones a los mismos IP Addresses, sólo una conexión a este IP se establece y la actual identidad derivada del certificado enviado por el servidor de destino debe hacer juego uno del nombre de estas rutas.

- Si la ruta S TP existe para los dominios receptores pero se ha configurado como dirección IP, la ruta sigue siendo uso de hacer una conexión pero una actual identidad del certificado se compara contra el dominio receptor y más futuro con el nombre de host derivado del registro de recursos DNS/MX.

Cuando hablamos de TLS requerido verifique la opción para los dominios recibidos, la manera cómo el ESA ha conectado con un servidor de destino es importante para el proceso de verificación de TLS debido a las rutas explícitamente configuradas S TP que proporciona la identidad adicional de la referencia que se considerará en el proceso.



el ~= representa la coincidencia exacta o del comodín

Ejemplo:

Tomemos un ejemplo a partir de la vida real, pero para el dominio receptor: example.com. Debajo del mí intenté describir todo el paso que son necesarios verificar manualmente la identidad del servidor.

Primero, recopilemos toda la información requerida sobre el servidor receptor.

Nombres 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: los nombres de host MX y los nombres del revDNS no hacen juego en este caso

Ahora deja para conseguir certificado una actual identidad:

IDENTIDADES DE LOS 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 servidores de destino hacen el mismo certificado instalar. Revisemos dos opciones de la validación y comparar la verificación resulta.

En caso de usar **TLS requerido verifique:**

La sesión de TLS se establece con uno de los servidores MX y la validación de la identidad comienza marcando la actual identidad deseada:

- actual identidad: **el dNSName existe** (continúe con comparar con la identidad permitida de la referencia)

  la identidad de la referencia = dominio receptor (**example.com**) se marca y **no hace juego el dNSName DNS: *.emailhosted.not, DNS: emailhosted.not**

- actual identidad: **El CN existe** (continúe con después actual identiy en cuanto el anterior no había coincidencia)

  la identidad de la referencia = dominio receptor (**example.com)** se marca y **no hace juego el CN *.emailhosted.not**

  identidad de la referencia = PTR(IP): una interrogación PTR se realiza contra el IP del servidor al cual el cliente de TLS (ESA) tiene conexión establecida y recibido un certificado, y de las devoluciones de esta interrogación: **mx0a.emailhosted.not.**

  El estado coherente DNS se marca para considerar este nombre de host como identidad válida de la referencia:

```
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
```

El valor de **mx0a.emailhosted.not** se compara contra CN ***.emailhosted.not y** allí hace juego. El Domain Name PTR valida la identidad y como el certificado es un certificado firmado de CA él valida el certificado entero y se establece la sesión de TLS.

En caso de usar **TLS requerido verifique para el dominio recibido** para este mismo beneficiario:

- actual identidad: **el dNSName existe** (así que el CN no será procesado en ese caso) se marca la identidad de la referencia = el dominio receptor (example.com) y
  no hace juego el dNSName DNS: *.emailhosted.not, DNS: emailhosted.notla identidad de la referencia = el FQDN (ruta smtp) - allí no es ningún smtproutes para este dominio receptor

  Como hay ningún SMTPROUTES usado además:

  la identidad de la referencia = el MX (dominio receptor) - una interrogación DNS MX se realiza contra el dominio receptor
  y devoluciones: **mx01.subd.emailhosted.not** - esto **no hace juego el dNSName DNS: *.emailhosted.not, DNS: emailhosted.not**
- actual identidad: **El CN existe pero se salta** mientras que existe el dNSName también.

Pues el CN no se considera ser procesado la validación de la identidad de TLS está fallando en ese caso así como la verificación del certificado y como consecuencia conexión no puede ser establecida.

Información Relacionada

- RFC6125 - https://tools.ietf.org/html/rfc6125
- RFC2818 - https://tools.ietf.org/html/rfc2818
- AsyncOS 8.0.2 Release Note
- Soporte Técnico y Documentación - Cisco Systems