CRE FAQ: ¿Cómo utilizo TLS para asegurar las contestaciones unencrypted CRE?

Contenido

[Introducción](#)
[¿Cómo utilizo TLS para asegurar las contestaciones unencrypted CRE?](#)
[Marco de políticas del remitente](#)
[Nombres de host y IP Addresses](#)
[Solución](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo utilizar Transport Layer Security (TLS) para asegurar las contestaciones del servicio del sobre registrado de Cisco (CRE), que permite que un usuario no necesite desencriptarlas, en asociación con el dispositivo de seguridad del correo electrónico de Cisco (ESA).

¿Cómo utilizo TLS para asegurar las contestaciones unencrypted CRE?

Por abandono, las contestaciones a un correo electrónico seguro son cifradas por los CRE y enviadas encendido a su mail gateway. Entonces pasan a través a sus servidores del correo cifrados para que el usuario final se abra con sus credenciales CRE.

Para evitar la necesidad del usuario de autenticar con los CRE para abrir la contestación segura, los CRE entregan en una forma “unencrypted” para enviar los gatewayes que soportan TLS. En la mayoría de los casos el mail gateway es el ESA, y este artículo se aplica.

Sin embargo, si hay otro mail gateway que se sienta delante del ESA tal como un filtro antispam externo, allí no es necesidad del certificate/TLS/mail fluye configuración en su ESA. En este caso, usted puede saltar los pasos 1 a 3 en la sección de soluciones de este documento. Para que las contestaciones unencrypted trabajen en este entorno, el filtro antispam externo (mail gateway) es el dispositivo que necesita soportar TLS. Si soportan TLS, usted puede hacer que los CRE confirmen esto y que le consigan configurado para las contestaciones “unencrypted” para asegurar los correos electrónicos.

Marco de políticas del remitente

Para evitar las fallas de verificación del Marco de políticas del remitente (SPF), usted debe agregar el MX: res.cisco.com, mxnat1.res.cisco.com, y mxnat3.res.cisco.com a su expediente SPF.

Donde y cómo usted agrega los CRE a su expediente SPF depende de cómo el Domain Name System (DNS) se implementa en su topología de red. Entre en contacto a su administrador de

DNS para más información.

Si el DNS no se configura para incluir los CRE, cuando es seguro componga y asegure las contestaciones se generan y entregado a través de los servidores dominantes recibidos, la dirección IP saliente no hará juego los IP Addresses mencionados en los beneficiarios termina, dando por resultado una falla de verificación SPF.

Nombres de host y IP Addresses

Hostname	IP Address	Tipo de registro
res.cisco.com	184.94.241.74	A
---- ---- ----	---- ---- ----	---- ---- ----
esa1.cres.iphmx.com	68.232.140.79	MX
esa2.cres.iphmx.com	68.232.140.57	MX
esa3.cres.iphmx.com	68.232.135.234	MX
esa4.cres.iphmx.com	68.232.135.235	MX
---- ---- ----	---- ---- ----	---- ---- ----
mxnat1.res.cisco.com	208.90.57.32	A
mxnat3.res.cisco.com	184.94.241.96	A

Los nombres de host y los IP Addresses están conforme al cambio basado en el servicio/el mantenimiento de red y mantienen/crecimiento de la red.

Solución

1. Obtenga y instale un certificado firmado y un certificado del intermedio en el ESA. **Note**: Es importante usted obtiene el certificado intermedio de su autoridad de firma como el certificado de la versión parcial de programa que viene en el dispositivo hace el proceso de verificación CRE fallar.
2. Cree una nueva directiva del flujo de correo: Del GUI, elija la **directiva de las directivas del correo > de las directivas del flujo de correo > Add….**Ingrese un nombre y deje todos otros en el valor por defecto a excepción de las *funciones de seguridad: TLS.* Fije esto a **requerido**.
3. Cree un nuevo grupo del remitente: Del GUI, elija el **grupo del remitente de las directivas del correo > de la descripción del SOMBRERO > Add….**Ingrese un nombre y fije el número de orden a #1. Usted puede también ingresar un comentario opcional. Elija la directiva del flujo de correo que usted creó en la licencia del paso 2. todo lo demás espacio en blanco.El tecleo **somete y agrega los remitentes >>**.
4. En el campo del remitente, ingrese estos rangos y los nombres de host IP:
   ```
   .res.cisco.com
   .cres.iphmx.com
   208.90.57.0/26 (current CRES IP network range)
   204.15.81.0/26 (old CRES IP network range)
   ```
5. Someta y confíe los cambios.
6. ¿Después de que usted se sienta confiado el ESA se prepara para TLS de los servidores CRE, sigue los pasos en cómo lo hace la prueba I si mi dominio soporta TLS con los CRE? para solicitar los servidores CRE para comenzar a utilizar TLS.

Información Relacionada

- ESA FAQ: ¿Cuáles son los IP y los nombres de host de los servidores dominantes CRE?
- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems