Configurar respuestas a mensajes del servicio de cifrado seguro de CRES mediante cifrado TLS

Contenido

Introducción

Este documento describe las acciones para configurar el cifrado TLS para las respuestas seguras entrantes de CRES en lugar de un adjunto de sobre seguro.

Cisco RES: Cómo Utilizar TLS para Proteger Respuestas RES No Cifradas

De forma predeterminada, Cisco RES cifra las respuestas a un correo electrónico seguro y las envía a su gateway de correo. A continuación, pasan a los servidores de correo cifrados para que el usuario final los abra con sus credenciales de Cisco RES.

Con el fin de eliminar la necesidad de autenticación de usuario al abrir una respuesta de mensaje seguro de Cisco RES, Cisco RES ofrece a los gateways de correo electrónico compatibles con la seguridad de la capa de transporte (TLS) en un formato "no cifrado". En la mayoría de los casos, el gateway de correo electrónico es el dispositivo de seguridad Cisco Email Security Appliance (ESA), y se aplica este artículo.

Sin embargo, si hay otro gateway de correo que se encuentra frente al ESA, como un filtro de spam externo, no es necesario el certificado/TLS/configuración de flujo de correo en su ESA. En este caso, puede omitir los pasos del 1 al 3 en la sección Solución de este documento. Para que las respuestas no cifradas funcionen en este entorno, el filtro de spam externo (gateway de correo electrónico) es el dispositivo que debe admitir TLS. Si son compatibles con TLS, puede hacer que Cisco RES lo confirme y le configure para respuestas "no cifradas" a correos electrónicos seguros.

Marco de políticas de remitente

Para evitar errores de verificación de Sender Policy Framework (SPF), agregue estos valores al registro SPF.

El valor de registro SPF de Cisco Registered Envelope Service (CRES) coincide con los nombres de host/IP de esta tabla, "Nombres de host y direcciones IP".

El resultado que utiliza el mecanismo SPF proporcionado por Cisco:

<#root>

```
~ dig txt
res.cisco.com
 +short
"v=spf1
mx:res.cisco.com


exists:%{i}.spf.res.cisco.com
 -all"
```

Agregue este mecanismo al registro SPF existente:

<#root>

```
include:res.cisco.com
```

Ejemplo de un registro SPF de prueba/FALSO que contiene el nuevo mecanismo res.cisco.com:

<#root>

```
"v=spf1 mx:sampleorg1.com ip4:1.2.3.4
include:res.cisco.com
 -all"
```

El lugar y el modo en que agregue Cisco RES al registro SPF depende de cómo se implemente el sistema de nombres de dominio (DNS) en la topología de red. Asegúrese de ponerse en contacto con el administrador de DNS para obtener más información.

Si DNS no está configurado para incluir Cisco RES, cuando se generan y entregan respuestas seguras y de redacción a través de los servidores de claves alojados, la dirección IP saliente no

coincide con las direcciones IP enumeradas al final del destinatario, lo que provoca un error de verificación SPF.

Nombres de host y direcciones IP

Hostname	IP Address	Tipo de registro
res.cisco.com	184.94.241.74	R
mxnat1.res.cisco.com	208.90.57.32	R
mxnat2.res.cisco.com	208.90.57.33	R
mxnat3.res.cisco.com	184.94.241.96	R
mxnat4.res.cisco.com	184.94.241.97	R
mxnat5.res.cisco.com	184.94.241.98	R
mxnat6.res.cisco.com	184.94.241.99	R
mxnat7.res.cisco.com	208.90.57.34	R
mxnat8.res.cisco.com	208.90.57.35	R
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

Nota: el nombre de host y las direcciones IP están sujetos a cambios según el mantenimiento de la red o el servicio o el crecimiento de la red. No todos los nombres de host y direcciones IP se utilizan para el servicio. Se proporcionan aquí como referencia.

Solución

- Obtenga e instale un certificado firmado y un certificado intermedio en el ESA.

> Nota: debe obtener el certificado intermedio de la autoridad de firma, ya que el certificado de demostración que se incluye en el dispositivo provoca un error en el proceso de verificación de CRES.

- Cree una nueva política de flujo de correo:
  a. En la GUI, seleccione Mail Policies > Mail Flow Policies > Add Policy.

    - Introduzca un nombre y deje todo lo demás por defecto excepto 'Funciones de seguridad: TLS'. *Defina este parámetro en* **Required**.

- Cree un nuevo grupo de remitentes:

  a. En la GUI, seleccione Mail Policies > HAT Overview > Add Sender Group.

    - Introduzca un nombre y establezca el número de pedido en #1. También puede introducir un comentario opcional. Elija la política de flujo de correo que creó en el paso 2. Deja todo en blanco.

    - Haga clic en Submit yAdd Senders.

- En el campo Sender, ingrese estos rangos de IP y hostnames:

```
.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)
```

-

Envíe y confirme los cambios.

- Después de estar seguro de que el ESA está preparado para negociar el cifrado TLS de los servidores Cisco RES, siga los pasos del portal de administración de CRES. ¿Cómo puedo probar si mi dominio admite TLS con Cisco RES?

Información Relacionada

- Cisco RES: direcciones IP y nombres de host para servidores de claves
- Dispositivo de seguridad Cisco Email Security Appliance: guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).