Contenido

Pregunta

¿Cómo proporciono el TAC de Cisco con el Acceso Remoto o soporto el túnel a un dispositivo de seguridad del correo electrónico o de la red de Cisco?

Entorno

Dispositivo de seguridad del correo electrónico de Cisco (ESA), Seguridad Appliance(WSA) de la red de Cisco

Los dispositivos de seguridad del correo electrónico/de la red de Cisco pueden utilizar un túnel seguro de SSH para permitir que el TAC de Cisco acceda al sistema operativo de los dispositivos. Por abandono, el dispositivo no permite este tipo de conexión (el Acceso Remoto del significado se inhabilita por abandono).

Usted puede habilitar esto vía el CLI o el GUI. Vea por favor las instrucciones abajo:

Del CLI

```
ESA.example.com> techsupport

Service Access currently disabled.
Serial Number: <S/N of the appliance>

Choose the operation you want to perform:
```

- SSHACCESS - Permita que un representante del servicio al cliente acceda remotamente su sistema,
  sin el establecimiento de un túnel.
- TÚNEL - Permita que un representante del servicio al cliente acceda remotamente su sistema,
  y establezca un túnel seguro para la comunicación.
- ESTATUS - Visualice el estatus actual del techsupport.
  []> túnel

Ingrese una contraseña temporal para que el soporte de cliente utilice. Esta contraseña no podrá ser utilizado para acceder directamente su sistema.

- La contraseña debe estar entre 6 y los caracteres 128 de largo.
- No puede ser espacio en blanco o consistir solamente en los espacios.
- Debe ser diferente de la contraseña del administrador.
  []> ***<supportpassword>***

```
Enter the port number for tunnel connection:
[25]> <Specify port or press Enter>

Are you sure you want to enable service access? [N]> Y

Service access has been ENABLED. Please provide your temporary password to your
Cisco Customer Support representative.

Waiting for ssh tunnel to connect, Ctrl-C to cancel...
```

Del GUI

Vaya **"a ayudar y a soportar"** *(la esquina superior derecha)* --> **"Accesos Remotos** bajo "Soporte técnico".

1. Haga clic **"editan el** botón de las **configuraciones del Acceso Remoto"**.
2. Ingrese una contraseña en **"el** campo de la **contraseña del soporte de cliente"**.
3. Marque el "túnel seguro (recomendado): la" opción y ingresa un número del puerto. El valor por defecto es 25.
4. Haga clic "**someten**" el botón.
5. Proporcione la contraseña elegida al TAC de Cisco.

El TAC de Cisco podrá tomar el control del dispositivo después de que usted haya proveído de ellos su número de serie y contraseña temporal. Todos los datos se transfieren con seguridad (usando el cifrado) y no se pueden leer por ningún partido otros entonces personales del TAC de Cisco. Si el dispositivo de seguridad del correo electrónico/de la red de Cisco no puede conectar sobre S TP (puerto TCP 25), después los otros puertos disponibles son 22, 80, 443, y 4766.

Nota: En las últimas versiones de AsyncOS, hemos realizado los cambios abajo en la sección del "Acceso Remoto" para los propósitos de seguridad complementaria:

- La contraseña ahora se refiere como ***"cadena del germen"***.
- Hay una opción para generar una cadena al azar del germen: Esto creará la clave más alta al azar del bit que será utilizada como la contraseña para la conexión de acceso remoto.
- Longitud de la cadena de la contraseña/del germen: La contraseña debe estar entre 12 y los caracteres 128 de largo.