Configuración de los parámetros de autenticación del servidor SSH en un switch a través de la CLI

Introducción

Secure Shell (SSH) es un protocolo que proporciona una conexión remota segura a dispositivos de red específicos. Esta conexión proporciona una funcionalidad similar a una conexión Telnet, excepto que está cifrada. SSH permite al administrador configurar el switch a través de la interfaz de línea de comandos (CLI) con un programa de terceros.

El switch actúa como un cliente SSH que proporciona capacidades SSH a los usuarios dentro de la red. El switch utiliza un servidor SSH para proporcionar servicios SSH. Cuando se inhabilita la autenticación del servidor SSH, el switch toma cualquier servidor SSH como de confianza, lo que disminuye la seguridad en su red. Si el servicio SSH está habilitado en el switch, la seguridad se mejora.

Este artículo proporciona instrucciones sobre cómo configurar la autenticación de servidor en un switch administrado a través de la CLI.

Dispositivos aplicables

- Serie Sx300
- Serie Sx350
- Serie SG350X
- Serie Sx500
- Serie Sx550X

Versión del software

- 1.4.7.06 - Sx300, Sx500
- 2.2.8.04: Sx350, SG350X, Sx550X

Configuración de los parámetros del servidor SSH

Configurar la configuración de autenticación del servidor SSH

Paso 1. Inicie sesión en la consola del switch. El nombre de usuario y la contraseña predeterminados son cisco/cisco. Si ha configurado un nuevo nombre de usuario o contraseña, introduzca las credenciales en su lugar.

Nota: Para saber cómo acceder a una CLI de switch SMB a través de SSH o Telnet, haga clic aquí.

```
User Name:cisco
Password:**********
```

Nota: Los comandos pueden variar dependiendo del modelo exacto de su switch. En este ejemplo, se accede al switch SG350X a través de Telnet.

Paso 2. Desde el modo EXEC privilegiado del switch, ingrese el modo de configuración global ingresando lo siguiente:

```
SG350X#configure
```

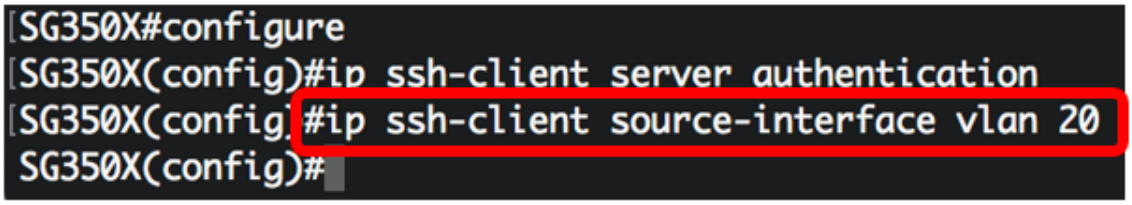
Paso 3. Para habilitar la autenticación del servidor SSH remoto por el cliente SSH, introduzca lo siguiente:

```
SG350X(config)#ip ssh-client server authentication
```

Paso 4. Para especificar la interfaz de origen a la que se utilizará la dirección IPv4 como dirección IPv4 de origen para la comunicación con los servidores SSH IPv4, introduzca lo siguiente:

```
SG350X(config)#ip ssh-client source-interface [interface-id]
```

- interface-id - Especifica la interfaz de origen.



Nota: En este ejemplo, la interfaz de origen es VLAN 20.

Paso 5. (Opcional) Para especificar la interfaz de origen cuya dirección IPv6 se utilizará como dirección IPv6 de origen para la comunicación con los servidores SSH IPv6, introduzca lo siguiente:

```
SG350X(config)#ipv6 ssh-client source-interface [interface-id]
```

- interface-id: especifica la interfaz de origen.

Nota: En este ejemplo, la dirección IPv6 de origen no está configurada.

Paso 6. Para agregar un servidor de confianza a la tabla de servidor SSH remoto de confianza, introduzca lo siguiente:

```
SG350X(config)#ip ssh-client server fingerprint [host | ip-address] [huella digital]
```

Los parámetros son:

- host: nombre de servidor de nombres de dominio (DNS) de un servidor SSH.
- ip-address - Especifica la dirección de un servidor SSH. La dirección IP puede ser una

dirección IPv4, IPv6 o IPv6z.
- huella digital - Huella digital de la clave pública del servidor SSH (32 caracteres hexadecimales).

```
SG350X#configure
SG350X(config)#ip ssh-client server authentication
SG350X(config)#ip ssh-client source-interface vlan 20
SG350X(config)#$00.1 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8
SG350X(config)#
```

Nota: En este ejemplo, la dirección IP del servidor es 192.168.100.1 y la huella dactilar utilizada es 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8.

Paso 7. Ingrese el comando **exit** para volver al modo EXEC privilegiado:

```
SG350X(config)#exit
```

```
SG350X#configure
SG350X(config)#ip ssh-client server authentication
SG350X(config)#ip ssh-client source-interface vlan 20
SG350X(config)#$00.1 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8
SG350X(config)#exit
SG350X#
```

Paso 8. Para mostrar los parámetros de autenticación del servidor SSH en el switch, introduzca lo siguiente:

```
SG350X#show ip ssh-client server [host | ip-address]
```

Los parámetros son:

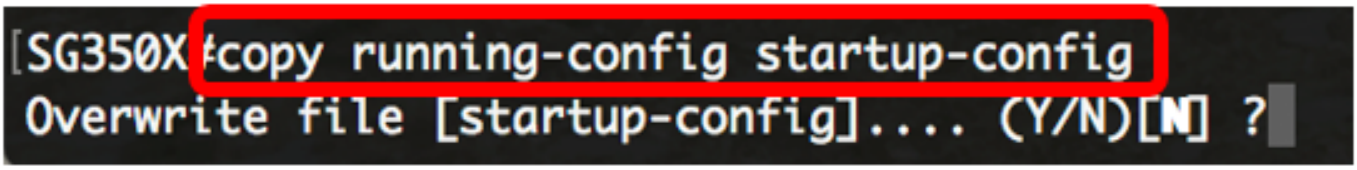
- host: nombre de servidor de nombres de dominio (DNS) de un servidor SSH.
- ip-address - Especifica la dirección de un servidor SSH. La dirección IP puede ser una dirección IPv4, IPv6 o IPv6z.

```
SG350X(config)#exit
SG350X#show ip ssh-client server 192.168.100.1
SSH Server Authentication is Enabled

Server address             : 192.168.100.1
  Server Key Fingerprint   : 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8


SG350X#
```

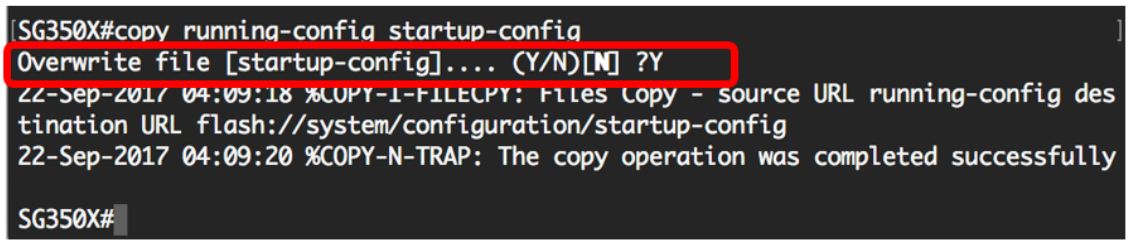
Nota: En este ejemplo, se ingresa la dirección IP 192.168.100.1 del servidor.

Paso 9. (Opcional) En el modo EXEC privilegiado del switch, guarde los parámetros configurados en el archivo de configuración de inicio introduciendo lo siguiente:

```
SG350X#copy running-config startup-config
```



Paso 10. (Opcional) Presione **Y** para Sí o **N** para No en su teclado una vez que el archivo Overwrite [startup-config].... aparece el mensaje.



Ahora ha aprendido los pasos para configurar la autenticación del servidor en un switch administrado a través de la CLI.