Sistema operativo extensible de FirePOWER (FXO) 2.2: Autenticación y autorización del chasis para la administración remota con el ACS usando el TACACS+.

Contenido

Introducción

Este documento describe cómo configurar autenticación de TACACS+ y autorización para el chasis extensible del sistema operativo de FirePOWER (FXO) vía el Access Control Server (ACS).

El chasis FXO incluye los rol del usuario siguientes:

- Administrador - Acceso de lectura y escritura completo al sistema entero. La cuenta de administración predeterminada se asigna este papel por abandono y no puede ser cambiada.
- Solo lectura - Acceso de sólo lectura a la configuración del sistema sin los privilegios de modificar al Estado del sistema.
- Operaciones - Acceso de lectura y escritura a la configuración del NTP, a la configuración elegante del Call Home para Smart que autoriza, y a los registros del sistema, incluyendo los servidores de Syslog y los incidentes. Acceso de lectura al resto del sistema.
- AAA - Acceso de lectura y escritura a los usuarios, a los papeles, y a la configuración AAA. Acceso de lectura al resto del sistema.

Vía el CLI esto puede ser vista como sigue:

fpr4120-TAC-A /security * # **papel de la demostración**

Papel:

Priv del nombre de la función

---------- ----

aaa aaa

admin admin

operaciones de las operaciones

solo lectura solo lectura

Contribuido por Tony Remirez, Jose Soto, ingenieros de Cisco TAC.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del sistema operativo extensible de FirePOWER (FXO)
- Conocimiento de la configuración de ACS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 2.2 del dispositivo de seguridad de Cisco FirePOWER 4120
- Versión 5.8.0.32 virtual del Access Control Server de Cisco

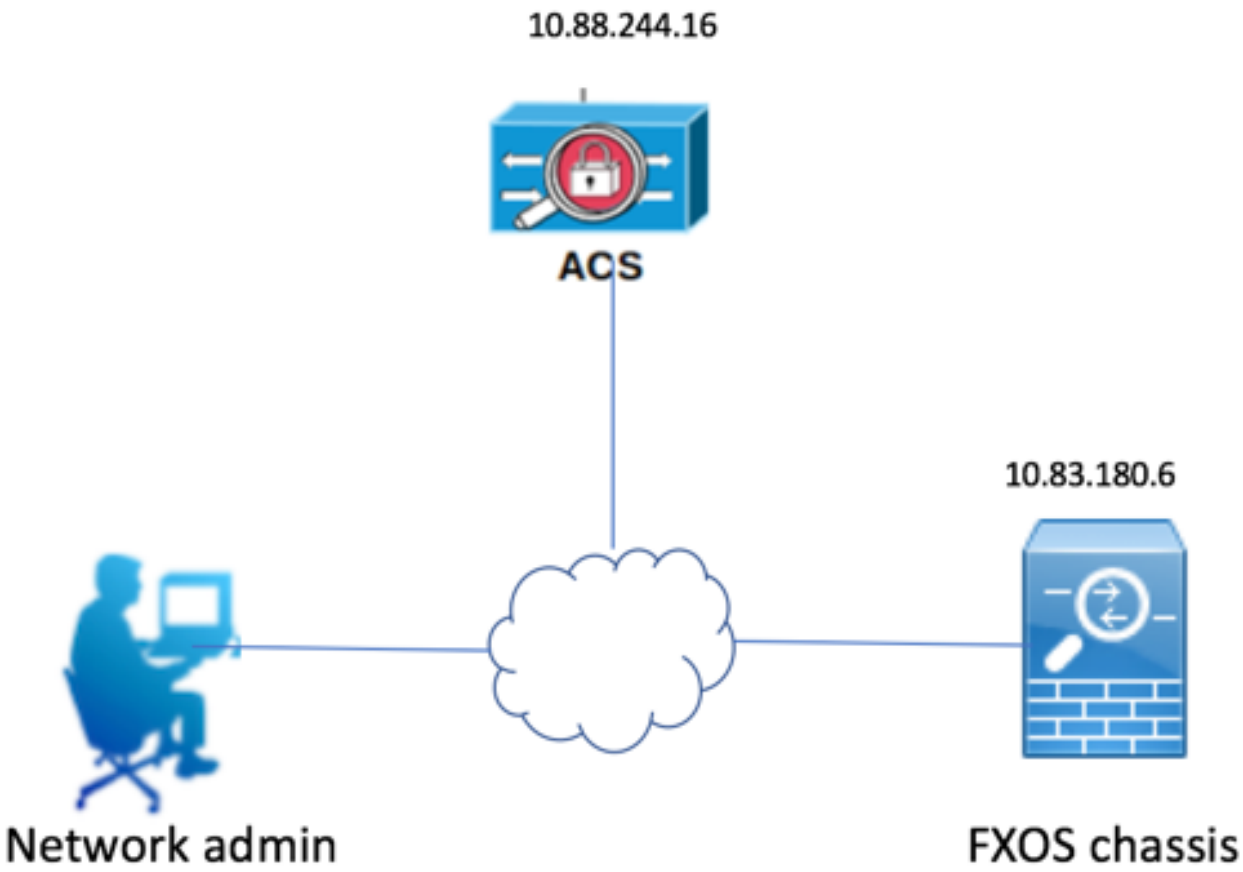
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

La meta de la configuración está a:

- Autentique el registro de usuarios en el GUI basado en web y SSH FXOS mediante el ACS.
- Autorice el registro de usuarios en el GUI basado en web y SSH FXOS según su rol del usuario respectivo mediante el ACS.
- Verifique la operación correcta de la autenticación y autorización en los FXO mediante el ACS.

Diagrama de la red



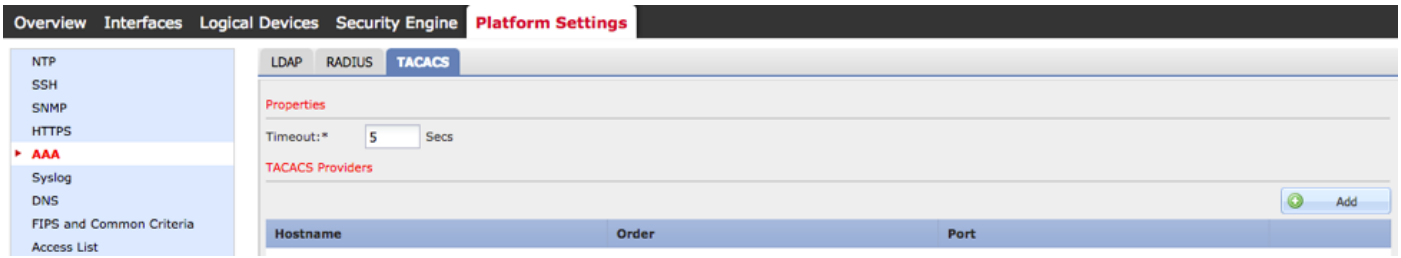
Configuraciones

Configurar el chasis FXO

Crear un proveedor TACACS que usa al administrador del chasis

Paso 1. Navegue a las **configuraciones de la plataforma >AAA.**

Paso 2. Haga clic la lengueta **TACACS**.

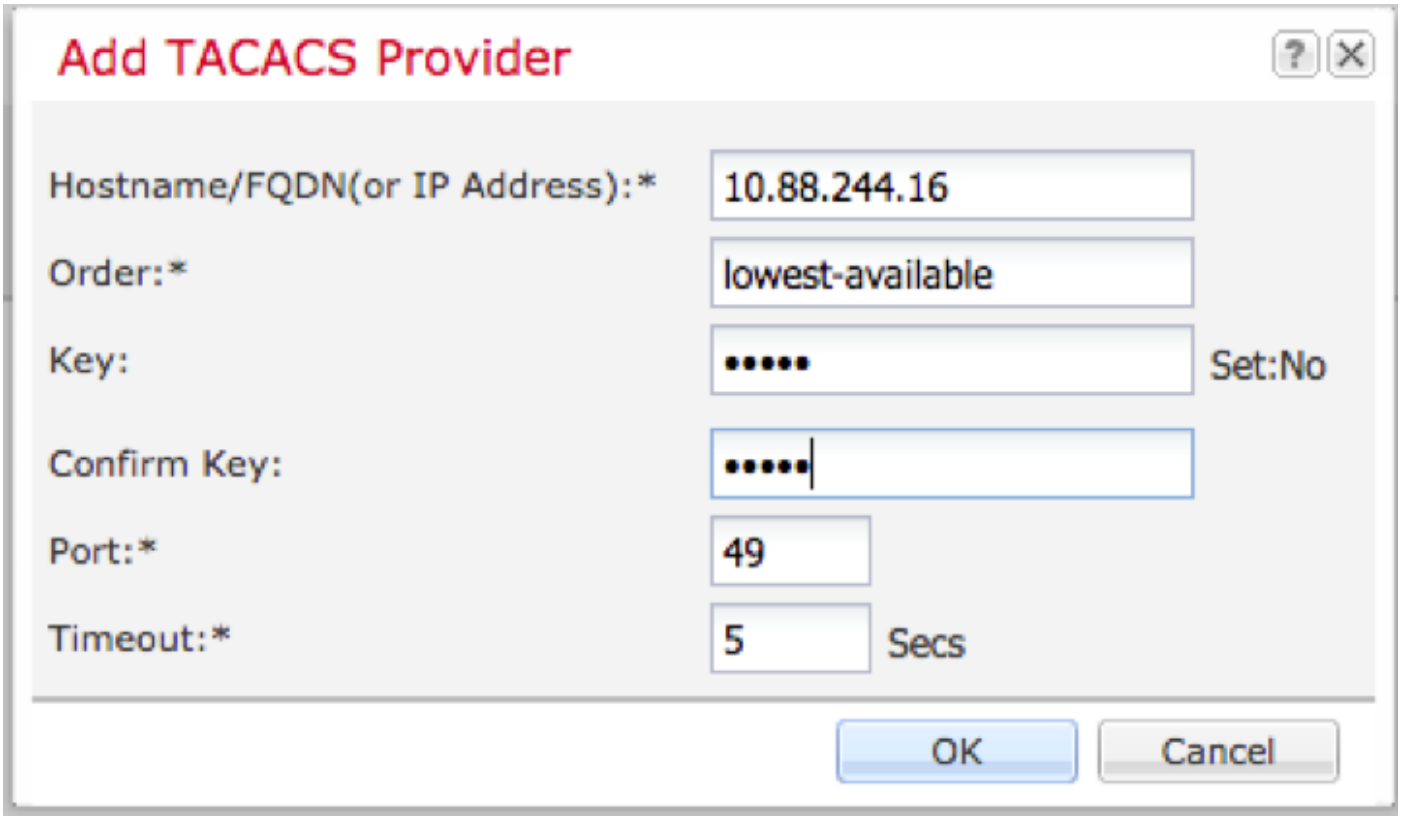


Paso 3. Para cada proveedor TACACS+ que usted quiere agregar (hasta 16 proveedores).

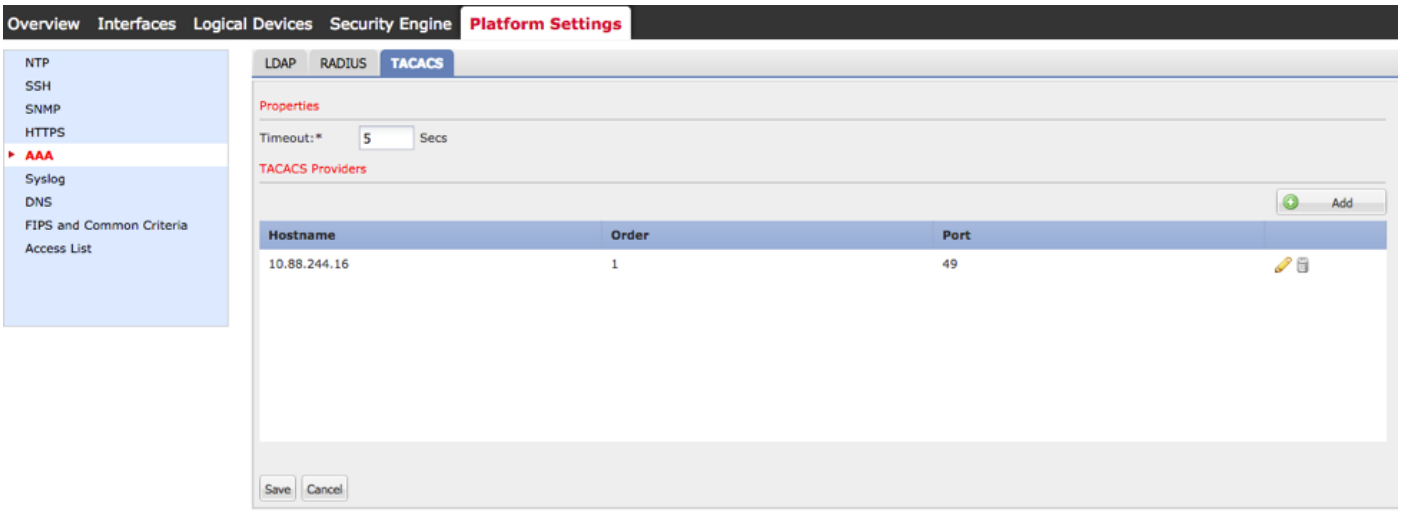
3.1. En el área de los proveedores TACACS, haga click en Add

3.2. En el cuadro de diálogo del proveedor del agregar TACACS, ingrese los valores requeridos.

3.3. Haga Click en OK para cerrar el cuadro de diálogo del proveedor del agregar TACACS.

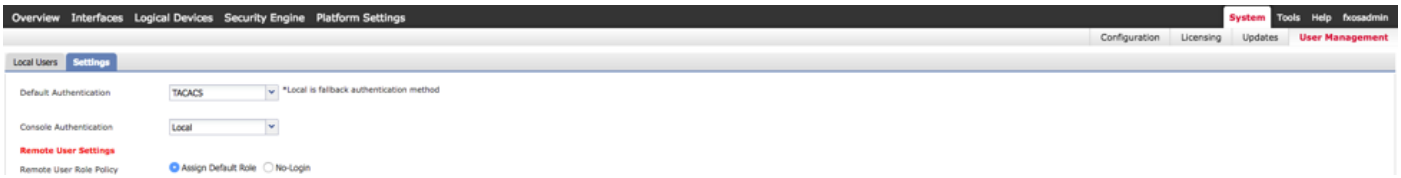


Paso 4. **Salvaguardia del** tecleo.



Paso 5. Navegue al **sistema > User Management (Administración de usuario) > las configuraciones**.

Paso 6. Bajo autenticación predeterminada elija el **TACACS**.



Crear un proveedor TACACS+ que usa el CLI

Paso 1. Para habilitar la autenticación de TACACS funcione con los siguientes comandos.

Seguridad del alcance fpr4120-TAC-A#

fpr4120-TAC-A /security # valor por defecto-**auth del alcance**

fpr4120-TAC-A /security/default-auth # **fijó los tacacs del reino**

Paso 2. Utilice el **comando detail de la demostración** de visualizar los resultados.

fpr4120-TAC-A /security/default-auth # **detalle de la demostración**

Autenticación predeterminada:

Reino Admin: **Tacacs**

Reino operativo: **Tacacs**

La sesión web restaura el período (en los secs): 600

Tiempo de espera de la sesión (en los secs) para la red, ssh, sesiones telnets: 600

Tiempo de espera de la sesión absoluto (en los secs) para la red, ssh, sesiones telnets: 3600

Tiempo de espera de la sesión de la consola en serie (en los secs): 600

Tiempo de espera de la sesión absoluto de la consola en serie (en los secs): 3600

Grupo de servidores del Admin authentication (autenticación de administrador):

Grupo de servidor de autenticación operativo:

Uso del 2do factor: No

Paso 3. Para configurar los parámetros del servidor TACACS funcione con los siguientes comandos.

Seguridad del alcance fpr4120-TAC-A#

fpr4120-TAC-A /security # **tacacs del alcance**

fpr4120-TAC-A /security/tacacs # **ingresan el servidor 10.88.244.50**

fpr4120-TAC-A /security/tacacs/server # **fijó el descr "servidor ACS"**

fpr4120-TAC-A /security/tacacs/server * # **fije la clave**

Ingrese la clave: **********

Confirme la clave: **********

Paso 4. Utilice el **comando detail de la demostración** de visualizar los resultados.

fpr4120-TAC-A /security/tacacs/server * # **detalle de la demostración**

Servidor TACACS+:

Nombre de host, FQDN o dirección IP: 10.88.244.50

Descr:

Orden: 1

Puerto: 49

Clave: ****

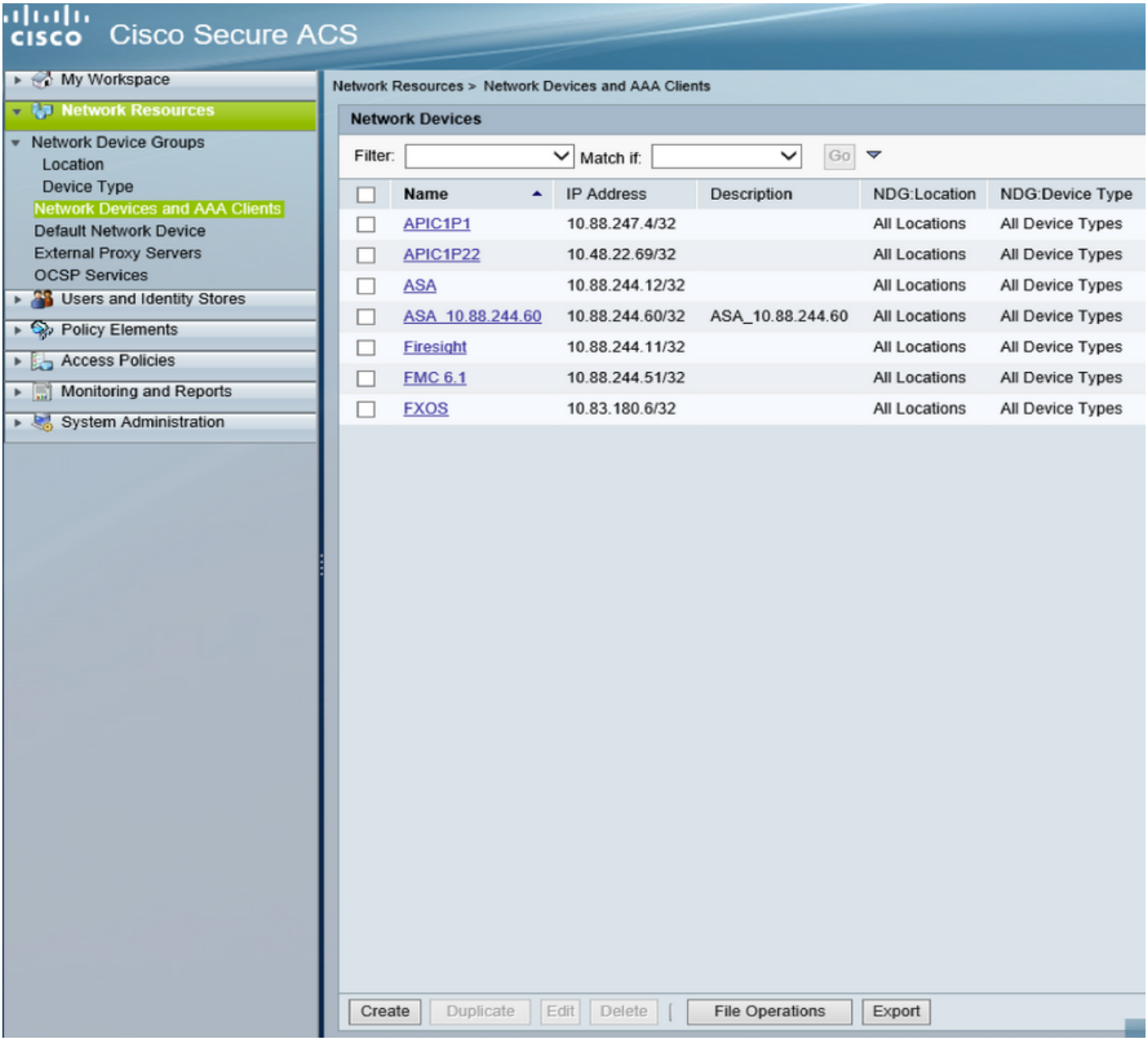
Descanso: 5

Configurar al servidor ACS

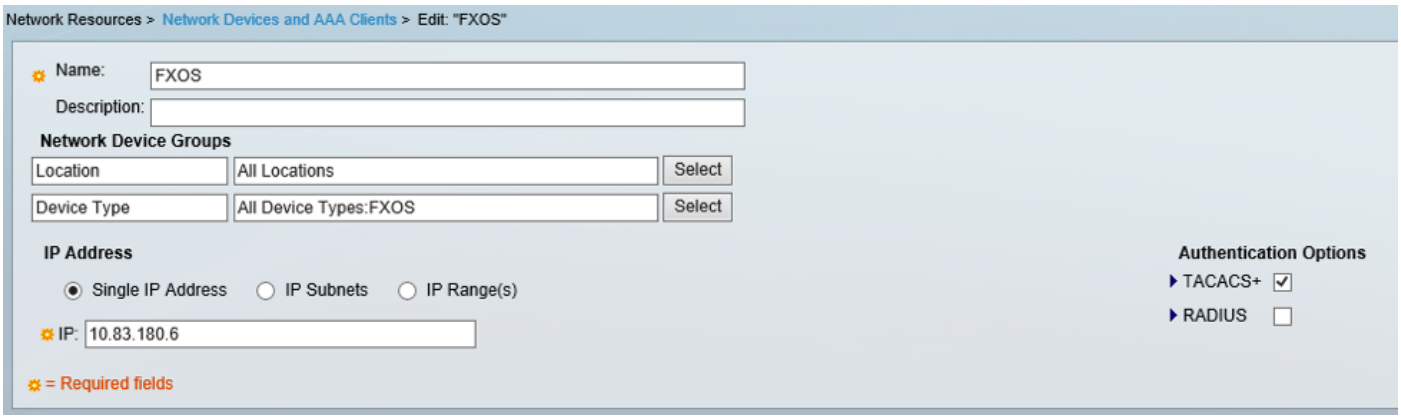
Agregar los FXO como recurso de red

Paso 1. Navegue a los **recursos de red > a los dispositivos de red y a los clientes AAA**.

Paso 2. El tecleo **crea.**



Paso 3. Ingrese los valores requeridos (el nombre, IP Address, tipo de dispositivo y habilita el TACACS+ y agrega la CLAVE).



Paso 4. El tecleo **somete.**