Preguntas frecuentes sobre seguridad contentas: ¿Cómo usted accede el CLI en un dispositivo de seguridad contento?

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[¿Cómo usted accede el CLI en un dispositivo de seguridad contento?](#)

Introducción

Este documento describe cómo acceder el CLI a través de un cliente de Telnet o del Secure Shell (SSH) en un dispositivo de seguridad del contenido de Cisco.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo de seguridad del correo electrónico de Cisco (ESA)
- Dispositivo de seguridad de la red de Cisco (WSA)
- Dispositivo de la Administración del Cisco Security (S A)
- AsyncOS

Componentes Utilizados

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

- Cisco ESA AsyncOS, todas las versiones
- Cisco WSA AsyncOS, todas las versiones
- Versiones AsyncOS de Cisco S A, todas las versiones

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.

> **Note**: Este documento se refiere al software que no es mantenido ni es soportado por Cisco. La información se proporciona como cortesía para su conveniencia. Para la asistencia adicional, entre en contacto por favor al proveedor de software.

¿Cómo usted accede el CLI en un dispositivo de seguridad contento?

Usted puede acceder el CLI de su dispositivo con un cliente Telnet o un cliente SSH. Sin embargo, el Telnet Protocol es unencrypted, así que cuando usted registra en su dispositivo con Telnet, sus credenciales puede se robe más fácilmente.

Cisco recomienda que todas las máquinas de la producción utilizan a un cliente SSH. Además, el cliente Telnet de Microsoft Windows del estándar es difícil de utilizar. Por el valor predeterminado de fábrica, Telnet se configura en el puerto de administración.

Complete estos pasos para inhabilitar Telnet:

1. Registro en la red GUI.
2. Navegue a la **red > a las interfaces IP**.
3. Haga clic el nombre de la interfaz que usted quiere editar.
4. Desmarque la casilla de verificación de **Telnet** en el campo de los servicios.

Complete estos pasos para acceder su dispositivo con SSH (puerto 22):

1. Instale a un cliente SSH en Microsoft Windows, tal como putty.
2. Inicie al cliente SSH:

   Agregue la información del host para su dispositivo (tal como **c650.example.com**).

   Haga clic la **carga**.

   Ingrese su nombre de usuario.

   Ingrese su contraseña.
3. Abra un comando prompt con el ***nix**.
4. Ingrese el comando de **exampleC650.com del ssh $**.
5. Si usted necesita especificar a un diverso usuario, ingrese el comando del **ssh**

<user>@exampleC650.com $. Si el Nombre de usuario es **admin**, ingrese el comando de **admin@C650.example.com del ssh $**.

Complete estos pasos para acceder su dispositivo con Telnet:

Note: Cisco recomienda que usted utiliza a un cliente SSH para el acceso; el uso de Telnet no se recomienda.

1. Abra un comando prompt.
2. Ingrese el comando **telnet c650.example.com**.
3. Ingrese su nombre de usuario.
4. Ingrese su contraseña.