Firewall seguro FTD Password Reset Tras la pérdida de contraseña

Problema

Firewall Threat Defence (FTD) se volvió inaccesible a través de CLI debido a la pérdida de una contraseña de administrador local. No se pudo tener acceso al nodo afectado con fines administrativos. La suposición inicial era que la contraseña de administrador se había cambiado desde el valor predeterminado y era desconocida, lo que provocaba la preocupación de que se necesitaría un restablecimiento de fábrica (recreación de imágenes) completo para restaurar el acceso y las credenciales predeterminadas. Se plantearon preguntas específicas sobre el procedimiento adecuado para tratar esta situación:

Entorno

- Firepower Management Center gestionado por Cisco Secure Firewall 1000, 2100 y 3100 FTD

Resolución

La resolución implicaba el intento de acceder al dispositivo FTD afectado utilizando las credenciales de administrador predeterminadas antes de continuar con el procedimiento más complejo de recreación de imágenes.

1: Antes de comenzar, intente iniciar sesión en el dispositivo FTD afectado con las credenciales de administración predeterminadas de fábrica.

```
Username: admin
Password: Admin123
```

Este paso se debe realizar en primer lugar, ya que podría eliminar la necesidad de más procedimientos de recuperación disruptivos.

2: Si se descartan las credenciales predeterminadas, restablezca la contraseña de administrador a un nuevo valor conocido mediante el procedimiento de cambio de contraseña de CLI de FTD estándar.

Proceso de recreación de imágenes: Guía de recreación de imágenes de Cisco Secure Firewall ASA y Threat Defence

- Realice una recreación de imágenes completa del dispositivo FTD afectado, siguiendo los pasos de la documentación de Cisco.
- Restaure las credenciales predeterminadas de fábrica mediante el proceso de recreación de imágenes.

Causa

La causa principal fue que la contraseña de administración del dispositivo FTD afectado nunca se había cambiado desde el valor predeterminado de fábrica durante la implementación inicial. La pérdida de acceso se debió a la suposición incorrecta de que la contraseña era desconocida, en lugar de una pérdida real de credenciales. El dispositivo siguió estando accesible utilizando las credenciales de administrador predeterminadas durante todo el incidente.

Contenido relacionado

- Sustitución de la unidad defectuosa en Firewall seguro Defensa frente a amenazas de alta disponibilidad
- Guía de solución de problemas de Cisco FXOS para la defensa frente a amenazas del firewall: Administración de imágenes
- Guía de recreación de imágenes de Cisco Secure Firewall ASA y Threat Defence
- Configuración, verificación y resolución de problemas del registro de dispositivos Firepower
- Configuración de alta disponibilidad de FTD en dispositivos Firepower
- Soporte técnico y descargas de Cisco

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).