Contenido

Introducción

Si usted registra en un host remoto que usa el protocolo del Escritorio Remoto (RDP), y el nombre de usuario remoto es diferente que su usuario, los sistemas cambia de FireSIGHT la dirección IP del usuario que se asocia a su dirección IP en el centro de administración de FireSIGHT. Causa el cambio en los permisos para el usuario en relación con las reglas del control de acceso. Usted notará que asocian al usuario incorrecto al puesto de trabajo. Este documento proporciona una solución para este problema.

Prerrequisitos

Cisco recomienda que usted tiene conocimiento en el sistema y el agente de usuario de FireSIGHT.

> Nota: 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.

Causa raíz

Este problema ocurre debido a los registros activos de Microsoft Directory(AD) de la manera que los intentos de autenticación RDP a la Seguridad de Windows abren una sesión el controlador de dominio. El AD registra el intento de autenticación para la sesión RDP contra la dirección IP del host de origen bastante que el punto final RDP que usted está conectando con. Si usted está registrando en el host remoto con una diversa cuenta de usuario, ésta cambiará al usuario asociado a la dirección IP de su puesto de trabajo original.

Verificación

Para verificar el es qué está ocurriendo, usted puede verificar que la dirección IP del evento de inicio de sesión de su puesto de trabajo original y el host remoto RDP tengan la misma dirección IP.

Para encontrar estos eventos, usted necesitará seguir los pasos abajo:

Paso 1: Determine el controlador de dominio contra el cual usted recibe está autenticando:

Ejecute el siguiente comando:

Salida de ejemplo:

La línea que comienza “DC: ” sea el nombre del controlador de dominio y la línea que el comienzo “dirige: ” la dirección IP.

Paso 2: Usando el registro RDP en el controlador de dominio identificado en el paso 1

Paso 3: Vaya al **Start (Inicio) > Administrative Tools (Herramientas administrativas) > Event Viewer**.

Paso 4: El taladro abajo a **Windows registra el > Security (Seguridad)**.

Paso 5: El filtro para la dirección IP de su puesto de trabajo haciendo clic el registro actual del filtro, haciendo clic la lengueta XML, y haciendo clic edita la interrogación.

Paso 6: Ingrese la interrogación siguiente XML, substituyendo su IP Address para <ip address>

Paso 7: Haga clic en el **evento de la conexión a la comunicación** y haga clic en la lengueta de los **detalles**.

Un ejemplo de salida:

Complete estos mismos pasos después de abrir una sesión vía el RDP y usted notará que usted recibirá otro evento de inicio de sesión (ID de evento 4624) con la misma dirección IP como se muestra por la siguiente línea de los datos XML del evento de inicio de sesión del inicio original:

Solución

Para atenuar este problema, si usted está utilizando el 2.1 del agente de usuario o arriba, usted puede excluir cualquier cuenta que usted lo vaya a hacer
está utilizando sobre todo para el RDP en la configuración de agente de usuario.

Paso 1: Registro en el host del agente de usuario.

Paso 2: Ponga en marcha la interfaz de usuario del agente de usuario.

Paso 3: Haga clic en la lengueta **excluida de los nombres de usuario**.

Paso 4: Ingrese todos los nombres de usuario que usted desea excluir.

Paso 5: Haga clic en Save (Guardar).

Los usuarios ingresados en esta lista no generan los eventos de la conexión a la comunicación en el centro de administración de FireSIGHT y no deben ser
asociado a los IP Addresses.