Acceso seguro ZTNA RDP Error de acceso a recursos privados para un recurso específico

Contenido

Problema

Los usuarios no pudieron acceder a un recurso privado RDP específico a través de Cisco Secure Access Zero Trust Network Access (ZTNA). Al intentar conectarse, los usuarios recibieron un mensaje de error interno. El problema afectó a varios usuarios, incluidos los nuevos usuarios agregados, e impidió que los usuarios que trabajan desde casa accedieran a los recursos de escritorio necesarios. Otros recursos de RDP y recursos privados no de RDP siguieron siendo accesibles, lo que indica que el problema era específico de esta configuración de recursos en particular.

Entorno

- Cisco Secure Access: acceso a la red sin confianza (ZTNA)
- Configuración de recursos privados con protocolo RDP
- Directivas de acceso basadas en grupos de Active Directory (AD)
- Varias configuraciones de recursos privados con direcciones IP superpuestas
- Evaluación del estado y la inscripción basada en el cliente

Resolución

El problema se resolvió identificando y corrigiendo conflictos de configuración en la configuración de recursos privados. Para resolver el problema, se tomaron los pasos descritos en las siguientes secciones.

Identificar conflictos de configuración

La investigación reveló que el recurso RDP específico se configuró bajo múltiples recursos privados: Inicie sesión en CSA Dashboard > Connect > End User connectivity > Under Zero Trust Access > Add a ZTA profile > Give it a Name, y luego busque un destino específico.

Eliminar asignaciones de direcciones IP en conflicto

La dirección IP 172.26.106.136 se quitó de los recursos privados en conflicto.

La dirección IP se dejó sólo en el recurso adecuado que coincidiera con los requisitos de directiva de acceso y pertenencia a grupos de Active Directory de los usuarios.

Verificar pertenencia de grupo de usuarios

Se confirmó que los usuarios recién agregados que experimentaban problemas de acceso no eran miembros del grupo de Active Directory (AD) correcto requerido para el acceso según la directiva de acceso configurada.

Además, asegúrese de que el grupo o usuario de AD correcto esté asociado al perfil de acceso de confianza cero.

Probar acceso después de cambios de configuración

Una vez implementados los cambios de configuración, los usuarios pudieron acceder correctamente al recurso RDP según fuera necesario. Se confirmó que el problema se había resuelto y que los usuarios podían conectarse sin recibir el mensaje de error interno.

Causa

La causa raíz del problema era un conflicto de configuración en el que el recurso específico se asignaba a varios recursos privados con diferentes directivas de acceso. Esto creaba una situación en la que los usuarios se evaluaban frente a directivas para las que no tenían la pertenencia de grupo de Active Directory adecuada, lo que resultaba en denegaciones de acceso y en el mensaje de "error interno ocurrido". Los usuarios recién agregados no eran miembros de los grupos AD correctos requeridos para las políticas en conflicto, lo que les impedía acceder al recurso aunque debían haber tenido acceso a través de la política apropiada.

Contenido relacionado

- 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).