Eliminación del perfil de acceso de confianza cero que causa la pérdida de acceso del usuario

Contenido

Problema

Después de eliminar un perfil de acceso de confianza cero (ZTA) que se creía que no se utilizaba, todos los usuarios con el módulo ZTNA experimentaron una pérdida total de acceso a los recursos privados y a la navegación por Internet. La eliminación de este perfil provocó una interrupción inmediata del servicio para todos los usuarios de ZTNA, lo que les impidió acceder a cualquier recurso a través de la infraestructura de acceso a la red de confianza cero.

Los usuarios afectados no pudieron establecer conexiones con:

- Recursos internos privados
- Navegación por Internet a través del módulo ZTNA

Entorno

- Acceso seguro (acceso a la red sin confianza)
- Módulo ZTNA implementado con varios perfiles de usuario
- Política predeterminada configurada con control ZTNA
- Varios perfiles ZTA configurados para la administración de acceso de usuarios

Resolución

Comprender la lógica de coincidencia de perfiles ZTA

Los perfiles de acceso de confianza cero se aplican en función de una lógica y un orden de coincidencia específicos:

- Orden de coincidencia de perfil: Los perfiles ZTA se evalúan en orden según los criterios de coincidencia de usuarios y destinos
- Comportamiento de perfil predeterminado: Cuando ningún perfil específico coincide con los criterios de usuario o de destino, el sistema vuelve al perfil predeterminado
- Dependencias de perfil: La eliminación de un perfil que actúa como predeterminado efectivo puede causar la interrupción del servicio aunque parezca que no se utiliza

Es probable que el perfil eliminado funcionara como el perfil predeterminado efectivo para la coincidencia de usuarios, a pesar de aparecer sin usar en la interfaz de configuración. Cuando se quitó este perfil, los usuarios perdieron su ruta de acceso principal a través de la infraestructura ZTNA.

Pasos de validación

Para evitar problemas similares en el futuro, es necesario implementar este enfoque de validación:

1.- Revisar todos los perfiles ZTA configurados y sus criterios de coincidencia antes de la eliminación.

2.- Identificar qué perfil sirve como predeterminado efectivo para el acceso de usuarios.

3.- Verificar la asignación de usuario a perfil a través de capturas de pantalla de configuración y revisión de políticas.

4.- Probar los cambios de perfil de forma controlada antes de aplicarlos a la producción.

Causa

La causa raíz fue la eliminación de un perfil ZTA que estaba funcionando como el perfil predeterminado efectivo para el acceso de usuario ZTNA, a pesar de aparecer sin usar en la interfaz de configuración. Cuando se quitó este perfil, el sistema perdió los criterios de coincidencia principales para el acceso de usuarios, lo que hizo que todos los usuarios de ZTNA perdieran la conectividad tanto con los recursos privados como con la navegación por Internet. La lógica de coincidencia de perfiles depende de que haya un perfil predeterminado válido disponible para reserva cuando otros perfiles configurados no cumplan los criterios específicos de usuario o destino.

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).