Problemas de Dirección del Tráfico ZTNA Basado en el Cliente con Secure Client

Contenido

Problema

El acceso a red de confianza cero (ZTNA) basado en cliente no puede proporcionar acceso a las aplicaciones internas cuando se accede mediante FQDN o dirección IP directa, mientras que las mismas aplicaciones siguen siendo accesibles a través de una conexión VPN.

Los síntomas específicos observados incluyen:

- Secure Client ZTNA no puede alcanzar las aplicaciones internas por FQDN o IP directa cuando VPN está desconectado.
- El acceso ZTNA basado en navegador funciona correctamente para las mismas aplicaciones.
- No aparecen eventos ZTNA en los registros de actividad cuando la VPN está inactiva, lo que indica que el tráfico del cliente no se está enrutando a través de la ruta ZTNA.
- Se ha comprobado que las definiciones de aplicaciones privadas coinciden con los recursos enrutables de VPN con las configuraciones correctas de IP/puerto/FQDN.
- Se ha confirmado que las políticas de ZTNA coinciden con las asignaciones de usuarios y grupos de prueba.

El problema se aísla específicamente en el mecanismo de control o aplicación del tráfico ZTNA de Secure Client, ya que el ZTNA basado en navegador valida que la publicación y aplicación back-end están funcionando correctamente.

Entorno

- Tecnología: Acceso seguro: acceso a la red sin confianza (ZTNA)

- Componentes: ZTNA basado en cliente, estado, inscripción, acceso a recursos privados
- Cliente seguro con perfiles de VPN coexistentes
- Aplicaciones privadas accesibles mediante FQDN y direccionamiento IP directo
- Funcionalidad ZTNA basada en navegador confirmada en funcionamiento
- Aplicación de políticas configurada en el modo de aplicación de coincidencias más específico

Resolución

La resolución implicaba ajustes de configuración del perfil ZTA y validación de políticas. Los pasos descritos en las siguientes secciones se han realizado para restaurar la funcionalidad ZTNA basada en cliente.

Paso 1: Agregar recursos privados al perfil ZTA

Se agregaron recursos privados a la configuración del perfil ZTA. Después de este cambio, los eventos bloqueados comenzaron a aparecer en los registros de actividad y las capturas de pantalla, lo que indica que el tráfico del cliente se estaba enrutando correctamente a través de la ruta ZTNA.

Paso 2: Verificación y prueba de políticas

Se agregó una regla temporal "permit any" para validar el flujo de tráfico. Mientras esta regla estaba activa, el acceso ZTNA basado en el cliente funcionaba correctamente, lo que confirmaba que el mecanismo de dirección del tráfico estaba funcionando, pero la aplicación de políticas necesitaba ajustes.

Paso 3: Perfeccionamiento de políticas

Se eliminó la regla permit-any temporal y se validaron las políticas de acceso específicas. Se

confirmó que se podía acceder al recurso privado con la política de acceso denominada Private Ressresources_Cyril mediante el modo de aplicación de coincidencias más específico de la plataforma.

Paso 4: Validación de configuración

El usuario confirmó que el acceso ZTNA basado en el cliente comenzó a funcionar de manera uniforme después de los cambios de configuración. El problema se resolvió sin necesidad de realizar modificaciones de políticas adicionales o cambios en el sistema.

Causa

La causa raíz fue la configuración incompleta del recurso privado en el perfil ZTA. Sin los recursos privados adecuados definidos en el perfil ZTA, el tráfico del cliente no se dirigía a través de la ruta de aplicación ZTNA, lo que provocaba que volviera a los mecanismos de routing locales. Esto dio lugar a que el tráfico eludiera por completo las políticas ZTNA, lo que explicó por qué no aparecían eventos ZTNA en los registros de actividad cuando se desconectaba VPN.

El problema era específico de la configuración de direccionamiento de tráfico ZTNA basada en cliente, mientras que ZTNA basada en navegador continuó funcionando porque utiliza un mecanismo de manejo de tráfico diferente que se configuró correctamente.

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).