Solicitudes DNS excesivas en el puerto 53 durante sesiones VPN de AnyConnect

Contenido

Problema

Después de implementar la VPN de acceso remoto (RA-VPN), los usuarios que se conectan a través de Cisco AnyConnect generan docenas de solicitudes DNS en el puerto 53 al servidor DNS secundario. Este comportamiento se observa en el Control de actividad para todos los usuarios conectados al túnel VPN y da lugar a numerosas solicitudes permitidas que inundan el túnel. Esta excesiva actividad de DNS no se produce cuando los usuarios se conectan a través de Zero Trust Access (ZTA), lo que indica que el problema está específicamente relacionado con el método de conexión VPN AnyConnect.

Entorno

- Familia de productos: Acceso seguro
- Instrumentación: Implementación de VPN de acceso remoto
- Entorno de comparación: Acceso de confianza cero (ZTA): no se experimenta el mismo comportamiento de inundación de DNS

Resolución

La investigación de las solicitudes de DNS excesivas requiere la recopilación y el análisis de registros para identificar la causa raíz del comportamiento de inundación de DNS. La recopilación de registros incluye la recopilación de captura de paquetes que incluye PID para cada paquete con el fin de determinar qué aplicación de un terminal está generando el tráfico y la salida del Monitor de procesos.

Causa

El análisis mostró que se esperaba esta cantidad de tráfico DNS.

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).