Desconexiones intermitentes de acceso seguro detrás de firewalls corporativos con errores IdleTimeout

Contenido

- Problema
- Entorno
- Resolución
  - Paso 1: Implemente la Configuración del Buffer TTL MX
  - Paso 2: Configurar exclusiones de dominio necesarias
  - Paso 3: Verificar las autorizaciones de puerto y protocolo
  - Paso 4: Supervisión y validación de la resolución
- Causa
- Contenido relacionado

Problema

Los clientes de Cisco Secure Access experimentan desconexiones intermitentes y reconexiones inmediatas cuando los terminales están conectados a la red corporativa. Las desconexiones se producen de forma aleatoria y el cliente se vuelve a conectar automáticamente transcurridos unos 5 segundos aproximadamente. Este comportamiento se observa cuando el tráfico de Internet pasa a través de Zero Trust Access (ZTA) a Secure Access desde los terminales situados detrás de los dispositivos Cisco FirePower y Meraki MX.

El registro de eventos de Windows captura errores específicos "idleTimeout" durante estos eventos de desconexión. El patrón de desconexión no se produce cuando los usuarios se

conectan desde conexiones de Internet domésticas, lo que indica que el problema está relacionado específicamente con la infraestructura de la red corporativa.

El síntoma provoca una interrupción en la empresa al proteger la conectividad de acceso remoto para los usuarios que operan en el entorno de red corporativo, mientras que los usuarios remotos no se ven afectados por este problema de conectividad.

Entorno

- Cisco Secure Access - Implementación de ventajas
- Software cliente Cisco Secure Internet Access (SIA)
- Infraestructura de red corporativa con appliances de seguridad Cisco FirePower
- Dispositivos de seguridad Meraki MX en la ruta de red
- Configuración de acceso de confianza cero (ZTA) que proxy el tráfico de Internet a acceso seguro
- Terminales de Windows con capacidad de registro de eventos
- Escenarios de conectividad mixtos: red corporativa (afectada) y conexiones domésticas a internet (no afectada)

Resolución

La resolución implicaba la implementación de cambios de configuración en el dispositivo Meraki MX y la garantía de las exclusiones de dominio y las asignaciones de puertos adecuadas para la integración de Secure Access.

Paso 1: Implemente la Configuración del Buffer TTL MX

Configure un búfer TTL MX en el dispositivo Meraki MX para abordar el comportamiento de almacenamiento en caché TTL DNS que estaba contribuyendo a los problemas de desconexión intermitente. Este cambio de configuración resuelve los conflictos de sincronización entre el

almacenamiento en caché de resolución DNS y las expectativas de conectividad del cliente Secure Access.

Paso 2: Configurar exclusiones de dominio necesarias

Asegúrese de que estos dominios se excluyen correctamente de la interceptación y se agregan a las listas sin descifrar en los dispositivos Cisco FirePower y Meraki MX:

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- Dominios de servicio de acceso seguro adicionales identificados en la configuración de políticas

Paso 3: Verificar las autorizaciones de puerto y protocolo

Configure la infraestructura del firewall corporativo para permitir los puertos y protocolos de acceso seguro necesarios a través de los dispositivos FirePower y Meraki MX. Asegúrese de que el tráfico al puerto 443 para los terminales del servicio Secure Access se maneje correctamente sin interferencias de la inspección de seguridad que podrían causar condiciones de tiempo de espera.

Paso 4: Supervisión y validación de la resolución

Después de implementar la configuración del búfer TTL MX, supervise el comportamiento del cliente Secure Access durante varios días para confirmar que el patrón de desconexión y reconexión intermitente ha cesado.

Causa

Las desconexiones intermitentes fueron causadas por conflictos de comportamiento de almacenamiento en caché DNS TTL (Time To Live) entre la infraestructura de red corporativa y

las expectativas del servicio Secure Access. El análisis de ingeniería de Cisco reveló que los valores TTL de DNS varían debido al comportamiento del almacenamiento en caché de la resolución, y se espera que las direcciones IP alternas se comporten debido a los mecanismos de equilibrio de carga en la arquitectura del servicio de acceso seguro.

Cuando los dispositivos de red corporativos (Cisco FirePower y Meraki MX) procesaban respuestas DNS para terminales de acceso seguro, el almacenamiento en caché y la gestión de TTL creaban discrepancias de tiempo que daban lugar a condiciones de "idleTimeout". Este conflicto de sincronización hizo que el cliente Secure Access interpretara la conexión como inactiva e iniciara ciclos de desconexión/reconexión.

El problema era específico de los entornos de red corporativos porque las conexiones domésticas a Internet normalmente no implementan el mismo nivel de almacenamiento en caché DNS y de inspección de tráfico que puede interferir con la administración del estado de conexión del cliente de acceso seguro.

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).