

Bloqueo incoherente de páginas tras la migración de Umbrella a Cisco Secure Access

Contenido

Problema

Después de migrar de Umbrella a Cisco Secure Access (SSE) mediante la herramienta de migración, el tráfico web bloqueado se redirige de forma incoherente a la antigua página de bloqueo de Umbrella en lugar de a la página de bloqueo de Cisco Secure Access. El problema ocurre con la defensa de DNS cuando diferentes dominios activan reglas de bloqueo, lo que da como resultado diferentes páginas de bienvenida y palabras de motivo de bloqueo. Esto crea notificaciones de bloqueo de usuario final incoherentes en toda la organización.

Los síntomas específicos observados incluyen:

- Las reglas de bloqueo redirigen a los usuarios a la antigua página de bloqueo de Umbrella en lugar de a la nueva página de bloqueo de Cisco Secure Access
- Diferentes dominios que activan reglas de bloqueo muestran diferentes páginas de bienvenida
- Texto de motivo de bloque incoherente presentado a los usuarios finales
- El comportamiento afecta a la funcionalidad de defensa de DNS después de la migración

Entorno

- Tecnología: Cisco Secure Access (SSE)
- Migración: Paraguas para SSE mediante la herramienta de migración
- Tipo de servicio: Defensa de DNS
- Implementación: Entorno posterior a la migración
- Escaneo web: Dispositivos FTD con análisis web activado

Resolución

El escaneo web en dispositivos FTD interfiere con la representación correcta de las páginas de inicio personalizadas para Cisco Secure Access. Para resolver este problema, omita el análisis web en los FTD para los tres dominios siguientes:

- `opendns.com`
- `cisco-secure.com`
- `sse.cisco.com`

Esta solución alternativa permite que las páginas de inicio de Cisco Secure Access personalizadas se representen correctamente en lugar de mostrar las páginas de bloqueo de Umbrella heredadas.

Pasos de verificación

Para comprobar la eficacia de la resolución:

Paso 1: Ejecutar pruebas de política para dominios que anteriormente mostraban un comportamiento incoherente

Paso 2: Verificar el comportamiento de bloqueo de la página después de implementar la solución alternativa

Confirme que el tráfico bloqueado ahora muestre de forma coherente la página de bloqueo de Cisco Secure Access en lugar de la página Umbrella antigua.

Paso 3: Validar redacción coherente de motivo de bloque

Asegúrese de que todos los dominios bloqueados ahora muestren mensajes de motivo de bloqueo uniformes alineados con los estándares de Cisco Secure Access.

Causa

El problema se debe a que la funcionalidad de análisis web de los dispositivos FTD interfiere con la correcta representación de las páginas de inicio personalizadas de Cisco Secure Access. Cuando el análisis web está activado en los FTD, impide la visualización correcta de las nuevas páginas de bloqueo, lo que hace que el sistema vuelva a las páginas de bloqueo de Umbrella anteriores. Esto crea experiencias de usuario incoherentes en las que diferentes dominios pueden activar diferentes formatos de páginas de bloqueo.

El equipo de ingeniería ha identificado este problema como un problema de nivel de diseño que requiere cambios desde la perspectiva de Talos. La arquitectura actual requiere que se omita el análisis web para dominios específicos de Cisco con el fin de garantizar una funcionalidad de página de inicio personalizada adecuada.

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).