

Búsqueda de actividad de Secure Access muestra nombres de reglas DESCONOCIDOS

Contenido

Problema

Durante una migración de Umbrella a SSE, los eventos de Búsqueda de actividad de Secure Access muestran el nombre de la regla como DESCONOCIDO en lugar de mostrar las reglas de políticas con nombre. Este comportamiento se observó para varios tipos de tráfico, incluido el tráfico permitido, como las solicitudes a chatgpt.com. La preocupación era si estas entradas de nombre de regla DESCONOCIDO indicaban un problema de configuración de política o un problema de migración que requería una solución.

Entorno

- Cisco Secure Access (SSE)
- Organización en proceso de migración de Umbrella a SSE
- Informes de Búsqueda de actividad de Secure Access
- Tráfico clasificado como dominios recién vistos

Resolución

El comportamiento Nombre de regla DESCONOCIDO es normal y se espera para los eventos gestionados por la lógica del sistema Secure Access en lugar de para las reglas creadas o nombradas por el cliente. Esto ocurre comúnmente para el tráfico categorizados como Dominios Recién Vistos, donde el dominio fue visto recientemente en el momento de la consulta y se informa como tal en los informes de Actividad de Búsqueda o Actividad de Seguridad.

Interpretación de Eventos de Búsqueda de Actividad con Nombres de Regla DESCONOCIDOS

Cuando encuentre eventos con Nombre de regla DESCONOCIDO, revise estos campos de evento para determinar el motivo de la aplicación y confirmar la aplicación de la política adecuada:

- Acción: muestra si se permitió o se bloqueó el tráfico
- Motivo del bloqueo de eventos / Motivo del bloqueo: proporciona detalles específicos de aplicación
- Categorías: muestra la categorización de contenido (como dominios recién vistos)
- Dominio/IP de destino: destino de la solicitud
- Identidad de usuario/origen: origen del tráfico
- Marca de tiempo: Cuándo se produjo el evento

Si el campo Categorías muestra Dominios recién vistos, se espera que UNKNOWN en el campo nombre de regla tenga un comportamiento y no indique un error en la migración o una corrupción de la política.

Pasos de validación para comportamiento inesperado

Si se esperaba que el tráfico coincidiera con una regla con nombre específica pero muestra UNKNOWN, recopile esta información para la validación de la trayectoria de política:

- 2-3 marcas de tiempo de eventos de ejemplo
- Dominio/IP de destino para cada evento
- Identidad de usuario/origen para cada evento

Esta información se puede utilizar para comparar la ruta de política esperada con el comportamiento real del evento y determinar si se requiere una investigación adicional.

Causa

El nombre de la regla UNKNOWN aparece cuando la lógica del sistema Secure Access procesa el tráfico en lugar de aplicar una regla de política creada/denominada por el cliente. Se trata de un comportamiento documentado para ciertas categorías de tráfico, en particular los dominios recién vistos, donde los mecanismos de gestión y categorización integrados tienen prioridad sobre las reglas con nombre durante la evaluación inicial del dominio.

Contenido relacionado

- [Habilitar seguridad de dominios recién vistos](#)
- [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).