

Solucionar problemas de entradas del registro de actividad DNS con decisión bloqueada

Contenido

Problema

Se notifican uno o más de estos síntomas:

- La búsqueda de actividad (Supervisión > Búsqueda de actividad, filtrada a eventos DNS) muestra Decisión/Acción = Bloqueado para un dominio, pero la revisión de las reglas de acceso a Internet no revela una regla que obviamente lo bloquee.
- El dominio no está presente en ninguna lista de destino de bloqueo que mantenga el administrador.

Entorno

- La información de este documento se basa en:
 - Plataforma en la nube Cisco Secure Access (SSE)
 - Cisco Secure Client 5.x con el módulo de seguridad de roaming implementado y registrado en una organización de acceso seguro

Resolución

Paso 1. Compruebe la identidad que se ha evaluado

- Confirme contra qué identidad se tomó la decisión. Si el evento muestra una identidad de red, sitio o túnel en lugar del equipo o usuario móvil esperado, la consulta coincidió con un conjunto de reglas distinto del revisado.
- En el caso de los usuarios de roaming, compruebe que el dispositivo está registrado y que informa que está protegido

Discordancia de identidad: Corrija la implementación de modo que se aplique la identidad deseada (registre el dispositivo móvil, corrija la asignación de AD/grupo de usuarios o ajuste el conjunto de reglas de identidad de red) en lugar de aflojar la regla que coincide incorrectamente.

Paso 2:Comprobar si hay una coincidencia de categoría de seguridad

- Si el evento incluye una categoría de seguridad (Malware, C2, Phishing, Dominios recién vistos, Tunelización DNS, etc.), el bloqueo procede de la configuración de seguridad del conjunto de reglas coincidente: no es necesario que ninguna lista de destino o regla de contenido haga referencia al dominio.
- Consulte la reputación y la categorización actuales del dominio en el portal Cisco Talos Intelligence en <https://talosintelligence.com/> (búsqueda del centro de reputación).
- Si la categorización o reputación mostrada en Talos es incorrecta, envíe una solicitud de disputa/reclasificación (abra un caso) con Talos directamente a través de <https://talosintelligence.com/> para que se reevalúe el dominio. Una vez que Talos actualiza la clasificación, el cambio se propaga a la aplicación de Secure Access.

Paso 3:Inspeccione la cadena CNAME

- Resuelva el dominio desde un punto de vista sin filtrar e inspeccione la cadena de respuesta completa (por ejemplo, `dig +noall +answer <domain> O nslookup -debug <domain>`).
- Verifique cada destino CNAME en la cadena contra las listas de destinos y contra la categorización Talos; un destino CNAME bloqueado explica una decisión Blocked en un dominio consultado aparentemente limpio

Paso 4:Volver a evaluar la política de arriba hacia abajo para la identidad real

- Recorra las reglas de acceso a Internet como la identidad del paso 1, comprobando el alcance de identidad de cada regla, programación, estado habilitado y configuración de seguridad/contenido/aplicación, hasta la regla predeterminada incluida.
- Utilice Policy Tester (por ejemplo, policy.test.sse.cisco.com/?=cisco.com) con la identidad y el destino exactos para ver qué regla de Secure Access informa como la coincidencia y compárela con la regla nombrada en el evento.

Caso especial: Dominios recién vistos

Si la categoría de seguridad del evento es Dominios recién vistos (NSD)

Opciones de remediación, por orden de preferencia:

Si el dominio es crítico para la empresa, agréguelo a una lista de permitidos destinos a la que haga referencia la regla aplicable; una entrada de permiso tiene prioridad sobre el bloque de seguridad NSD para ese destino.

Desactivar DNS cifrado (DoH) y QUIC

El cifrado de DNS y QUIC puede provocar lagunas en la visibilidad de la capa DNS, lo que puede generar confusión en los resultados de la búsqueda por actividad: las consultas resueltas sobre el navegador DoH nunca llegan a los resolvers de Secure Access (por lo que faltan por completo en el registro), mientras que los dominios del proveedor DoH pueden aparecer como eventos bloqueados.

La desactivación de estos transportes en los terminales gestionados garantiza que todos los DNS sigan siendo inspeccionables y que el registro de actividad refleje el comportamiento real de los terminales.

DNS sobre HTTPS (DoH) por navegador

Google Chrome

- Manual: Vaya a `chrome://settings/security` y desactive Use secure DNS.

Microsoft Edge

- Manual: Vaya a `edge://settings/privacy` y desactive Use secure DNS.

Mozilla Firefox

- Manual: Menú > Configuración > Privacidad y seguridad > DNS sobre HTTPS (o Configuración de red en versiones anteriores) y seleccione Desactivado / anule la selección de Activar DNS sobre HTTPS.
- Nota: Los resolvers de Umbrella/Secure Access responden al dominio canario de Mozilla (use-application-dns.net) de una manera que indica a Firefox que mantenga el DoH desactivado de forma predeterminada; la configuración explícita de GPO se sigue recomendando porque la configuración DoH establecida por el usuario invalida la comprobación canaria. Precaución: no agregue los dominios kill-switch/canary de Mozilla a una lista de destino de bloqueo: una respuesta de registro A de página de bloqueo se trata como válida y puede hacer que Firefox mantenga o actualice su uso de DoH.

QUIC (HTTP/3)

QUIC se ejecuta en UDP/443 y puede transportar tanto tráfico web general como DoH3 (DNS sobre HTTP/3), omitiendo las rutas de inspección que esperan TCP.

Al deshabilitar QUIC, los exploradores se ven obligados a recurrir a HTTP/2 o HTTP/1.1 basado en TCP, lo que restaura la visibilidad completa:

- Cromado/Borde: Manual (no persistente, modificable por el usuario): establezca `chrome://flags/#enable-quic` / `edge://flags/#enable-quic` en Disabled.
- Firefox: establezca la preferencia `network.http.http3.enable = false` (`about:config` o `policy/AutoConfig`).

Si, después de estos pasos, la regla coincidente notificada en el evento sigue sin poder conciliarse con la configuración, abra un caso con Cisco TAC y proporcione la exportación del evento de búsqueda de actividad (marca de tiempo con zona horaria, identidades, regla coincidente, categorías, tipo de registro y dominio) junto con capturas de pantalla de las reglas relevantes y las listas de destinos.

Causa

Coincidencia de categoría de seguridad (inteligencia de Talos): el dominio está bloqueado por una configuración de seguridad (por ejemplo, malware, comandos y control, suplantación de identidad, cifrado, tunelación DNS o dominios recién vistos) basada en la reputación y categorización de Cisco Talos, no por ninguna lista de destinos ni regla de contenido que el administrador haya configurado explícitamente. Esta es la causa más frecuente de los bloques "sin coincidencia obvia".

Discordancia de atribución de identidad: la consulta se atribuyó a una identidad diferente a la esperada (identidad de red/sitio en lugar del equipo móvil, un usuario/grupo de AD diferente o un dispositivo no registrado que vuelve a una política de nivel de red), por lo que se encontró una regla distinta (a menudo más estricta o predeterminada).

Orden de las reglas y regla predeterminada: una regla más amplia de la directiva (o la regla predeterminada/catch-all de la parte inferior) coincidió antes de la regla de permiso prevista; la regla deseada también se puede deshabilitar, programar o establecer el ámbito de las identidades que no incluyen el origen afectado.

Herencia de lista de destino: una lista de destino de bloqueo contiene un dominio principal (example.com), que cubre implícitamente todos los subdominios (app.example.com), o contiene una IP/CIDR a la que el dominio se resuelve. La búsqueda en las listas del FQDN exacto por sí sola no aparece.

Bloqueo de cadena CNAME: el dominio consultado está permitido, pero su cadena de resolución contiene un CNAME a un dominio (normalmente un CDN, un rastreador o un host estacionado/bloqueado) que está bloqueado; la decisión se aplica a la cadena y el registro muestra el dominio consultado originalmente como Bloqueado.

Coincidencia de aplicación o categoría de contenido: el dominio pertenece a una aplicación bloqueada (control de aplicación) o categoría de contenido que el administrador no asoció a ella; La categorización puede diferir de la intuición (por ejemplo, una herramienta empresarial clasificada como Uso compartido de archivos o Proxy/Anonimizador).

Cambio reciente de política o categorización - La política o la categorización Talos cambió recientemente; el evento objeto de revisión es anterior (o posterior) al cambio o a la propagación de directivas/sincronización del cliente que no se había completado en el momento de la consulta.

Contenido relacionado

- [Configurar servidores DNS internos para Umbrella](#)
- [Configuración de DNS sobre HTTPS \(DoH\) con Umbrella](#)
- [Agregar un controlador de dominio en Secure Access](#)
- [Información de la página de bloqueo de Cisco Secure Access](#)
- [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).