¿Por qué podría necesitar un proxy?

Si bien toda la detección y protección conductual del agente de Cyber Crucible ocurre en el endpoint, sin necesidad de enviar muestras a la nube para su análisis, el agente del endpoint aún requiere una conexión a un servidor para recibir información de licencia, configuración, actualizaciones de software, etc.

Si su red está restringida hasta el punto de no permitir conexiones a los rangos de IP donde se alojan los servidores de Cyber Crucible, es posible que necesite configurar un proxy para permitir que el agente (únicamente) alcance su servidor para la instalación. Consulte How to Manage Proxy Configurations para obtener información sobre cómo configurar el agente.

¿Qué tipo de proxy puedo usar?

A partir de la versión 4.4.6.3 del agente de Cyber Crucible, las configuraciones de proxy admiten Socks5. No existe restricción sobre dónde se aloja el servidor (en las instalaciones o externamente), siempre que las restricciones de red permitan que los agentes lo alcancen. A continuación se muestra un diagrama de ejemplo de una configuración de proxy simple donde el servidor Socks5 está alojado dentro de la red restringida, y solo tiene permitido conectarse a una máquina externa que canaliza el tráfico.

SOCKS5H.png

Esta configuración permite que los agentes se conecten a sus servidores, manteniendo al mismo tiempo la política de red. Solo requiere 1 regla que permita al host Socks5 alcanzar su servidor proxy externo en un puerto (ssh). Esto asegura que no solo todo el tráfico va por el puerto 443, sino que además está doblemente envuelto en SSH antes de salir de la red, y no requiere reenvío de puertos entrantes (port-forwarding).

Revision #1
Created 2026-07-24 01:31:03 UTC by Dennis Underwood
Updated 2026-07-24 01:31:03 UTC by Dennis Underwood