Pourquoi pourrais-je avoir besoin d'un proxy ?

Bien que toute la détection comportementale et la protection de l'agent Cyber Crucible s'effectuent au niveau du point de terminaison, sans nécessiter l'envoi d'échantillons vers le cloud pour analyse, l'agent du point de terminaison nécessite tout de même une connexion à un serveur pour recevoir les informations de licence, la configuration, les mises à jour logicielles, etc.

Si votre réseau est verrouillé au point de ne pas autoriser les connexions vers les plages IP où les serveurs Cyber Crucible sont hébergés, vous devrez peut-être configurer un proxy pour permettre à l'agent (uniquement) d'atteindre son serveur pour l'installation. Consultez Comment gérer les configurations de proxy pour obtenir des informations sur la configuration de l'agent.

Quel type de proxy puis-je utiliser ?

Depuis la version 4.4.6.3 de l'agent Cyber Crucible, les configurations de proxy prennent en charge Socks5. Il n'y a aucune restriction quant à l'endroit où le serveur est hébergé (sur site ou hors site), tant que les restrictions réseau permettent aux agents de l'atteindre. Un exemple de schéma est présenté ci-dessous illustrant une configuration proxy simple où le serveur Socks5 est hébergé au sein du réseau verrouillé, et n'est autorisé qu'à se connecter à une machine externe qui achemine le trafic en tunnel.

SOCKS5H.png

Cette configuration permet aux agents de se connecter à leur(s) serveur(s), tout en maintenant la politique réseau. Elle ne nécessite qu'une seule règle autorisant l'hôte Socks5 à atteindre son serveur proxy externe sur un seul port (ssh). Cela garantit non seulement que tout le trafic passe par le port 443, mais aussi qu'il est doublement encapsulé en SSH avant de quitter le réseau, sans nécessiter de redirection de port entrant.

Revision #1
Created 2026-07-24 06:38:34 UTC by Dennis Underwood
Updated 2026-07-24 06:38:34 UTC by Dennis Underwood