Why might I need a proxy?

While all of the Cyber Crucible agent’s behavioral detection and protection happens at the endpoint, without need to submit samples to the cloud for analysis, the endpoint agent still requires a connection to a server to receive licensing information, configuration, software updates, etc.

If your network is locked down to the point of not allowing connections to IP ranges where the Cyber Crucible servers are hosted, then you may need a proxy configured to allow the agent (only) to reach its server for installation. See How to Manage Proxy Configurations for information on configuring the agent.

What type of proxy can I use?

As of version 4.4.6.3 for the Cyber Crucible agent, the proxy configurations support Socks5. There is no restriction on where the server is hosted (on prem, or off), as long as the network restrictions allow the agents to reach it. An example diagram is given below of a simple proxy configuration where the Socks5 server is hosted within the locked down network, and is allowed only to connect to an external machine that tunnels traffic.

SOCKS5H.png

This setup allows the agents to connect to their server(s), while maintaining the network policy. Requiring only 1 rule that allows the Socks5 host to reach its external proxy server on one port (ssh). This ensures that not only is all traffic on 443, but also doubly wrapped in SSH before leaving the network, and requires no inbound port-forwarding.

Revision #4
Created 2026-05-18 20:28:11 UTC by Dennis Underwood
Updated 2026-07-20 19:21:48 UTC by Dennis Underwood