PROXY OVERVIEW

Proxies are often used in enterprise environments as a caching, filtering, and audit point for network connections between clients and servers (primarily "web" traffic). Proxy servers can handle outbound requests from systems for network resources, optionally caching web content and/or enforcing local site restriction policies. Historically, the connection to the proxy from the client system took place over HTTP, but initial proxy connections via HTTPS are becoming increasingly common.

A popular misconception is that you must connect to an HTTPS proxy to connect to HTTPS-enabled sites. This is not true. Most proxies can connect to both HTTP and HTTPS sites via the TCP CONNECT method, and in some cases can also handle additional protocols such as FTP.

Along with the initial access method to a proxy (HTTP/HTTPS), authentication is also frequently used to restrict access to the proxy system. Common forms of authentication used with proxies include Basic Authentication, Windows NTLM, Kerberos, and SAML.

Mandiant Security Validation supports various proxy types, grouped by initial access method and optional authentication type. You can select from the following proxy types when creating a proxy definition in the Validation platform:

- **http:** Uses HTTP as the access protocol to the proxy itself (where the initial connection is not encrypted). No authentication is required, so any client system not filtered at the network level can use this type of proxy. Connections to both HTTP and HTTPS sites (via CONNECT) are usually supported through the proxy, but local policy may further restrict access.
- **http_auth:** Uses HTTP as the proxy connection protocol but requires authentication (username and password). The user credentials are sent as Base64-encoded values over a non-encrypted HTTP connection. This method is known as Basic Authentication.
- **http_kerberos:** Also uses HTTP for proxy access with authentication, but instead of simple Base64 encoding of user credentials, an encrypted "service ticket" is passed to the proxy to authorize user access to the requested resource. Kerberos authentication is the most common authentication method used in Windows Active Directory environments, but it can also be used in non-Windows (e.g., Linux) environments independent of Active Directory. Kerberos is a more secure form of authentication but requires more configuration than other methods.
- **http_ntlm:** Uses HTTP for proxy access, but user authentication is performed via a "challenge/response" mechanism in which user credentials themselves are never sent across the network.

  

  NTLMv2 is a legacy authentication mechanism for Windows networks and is considered deprecated by Microsoft. Kerberos authentication is more commonly used in modern networks and recommended for new proxy installations.

- **https:** The connection to the proxy is over HTTPS (encrypted), but no authentication is performed. Connections to both HTTP and HTTPS sites are usually supported. The proxy will present a standard HTTPS certificate that the client may validate before using the proxy for connections.
- **https_auth:** Proxy connectivity occurs over HTTPS, but the proxy requires authentication (username and password). User credentials are sent as Base64-encoded values over the connection but are encrypted by the initial HTTPS connection to the proxy.
- **https_kerberos**: Also uses HTTPS for proxy access with authentication, but an encrypted "service ticket" is passed to the proxy to authorize user access to the requested resource. Kerberos authentication is the most common authentication method used in Windows Active Directory environments, but it can also be used in non-Windows (e.g., Linux) environments independent of Active Directory. Kerberos is a more secure form of authentication but requires more configuration than other methods.
- **http_https_auto:** Proxy connections are chosen as HTTP and HTTPS automatically based on the destination

protocol. No authentication is required.

- **http_https_auto_auth:** This is the same as the http_https_auto proxy type, but with Basic Authentication.
- **os_defined:** Supported on Windows systems only, proxy settings are detected automatically based on system registry configurations.
- **saml:** Normally used in Single Sign-On (SSO) environments, this proxy type employs the SAML standard for authentication by transferring identity data between service providers (e.g., MSV) and identity providers (e.g., Azure AD).
- **socks:** SOCKS is a general-purpose proxy type that supports tunneling for various types of protocol requests such as HTTP/HTTPS, POP3, SMTP, etc.
- **socks_auth:** This is similar to the SOCKS proxy; however, the proxy requires authentication before use.

  

  To support SOCKS with authentication, a minimum of SOCKS5 proxy type must be used.

- **ssl_mitm:** Connections to HTTPS sites are handled by the proxy server in a “man-in-the-middle” fashion, where the proxy terminates the HTTPS connection from the client, initiates a connection to the target server, and forwards traffic between the connections. With this configuration, the proxy server generates on-the-fly certificates for the client rather than passing the certificate received from the remote server. The client must be configured to import any transient certificates generated by the proxy as trusted certificates.

  

  The ssl_mitm proxy type can be configured to run in transparent mode, where traffic is routed through the proxy at the network layer without requiring any proxy configuration on the client (other than trusting any proxy-generated certificates).