SSL Exemptions Required for Use With Barracuda Content Shield Suite

https://campus.barracuda.com/doc/85493016/

The Barracuda Content Shield service uses certificate pinning to prevent malicious interference with SSL traffic between the Barracuda Content Shield Suite (endpoint machines) and the service. During the handshake that takes place when an SSL/TLS connection is established, the client (endpoint) can authenticate the server it is talking to by validating that the server certificate was issued by a Certificate Authority that the client trusts. Certificate pinning is the process of associating a host with their *expected* certificate or public key. Once a certificate or public key is known or seen for a host, the certificate or public key is associated with, or 'pinned' to, the host.

To avoid interruption to SSL traffic between the service and the endpoint machines with the suite installed, you must exempt the URL `api.bcs.barracudanetworks.com` from SSL Inspection by any device between the endpoints and the service.

For example, if you are using a Barracuda CloudGen Firewall, see SSL Inspection in the Firewall for details about how to create exceptions to SSL Inspection.