Test File Inspection with Eicar

Contents

Introduction

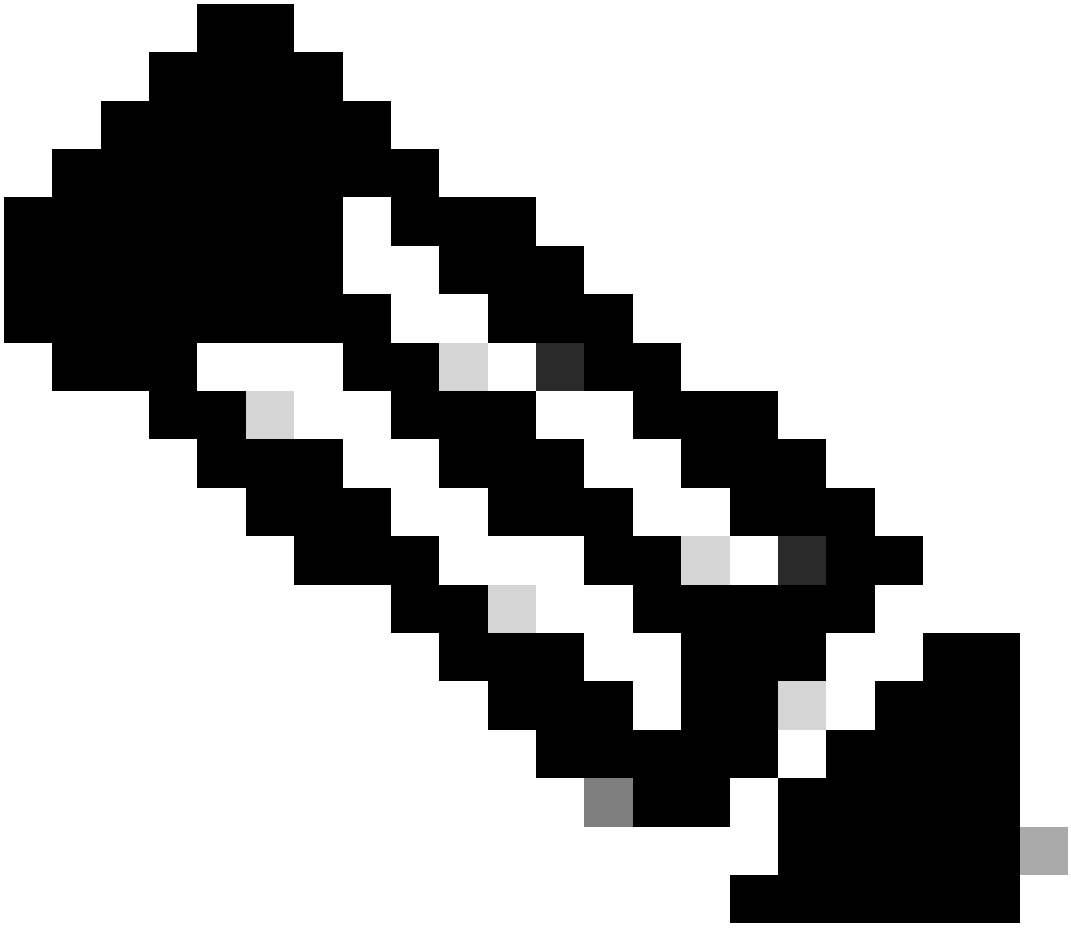
This document describes how to test file inspection with Eicar.

Overview

At present, when testing whether or not the File Inspection feature is enabled by using the eicar.org test download files, you see different behaviour when "SSL decryption" enabled or disabled. Umbrella File Inspection only AV scans downloads at eicar.org if SSL decryption is **enabled**.

Understanding the Detection Process For Eicar

To enable blocking of eicar.org, please enable SSL decryption.



Note: SSL Decryption is required even when visiting the site over HTTP. If you do not have SSL Decryption enabled, the proxy bypasses domains that serve traffic over HTTPS.

- The Umbrella Intelligent Proxy makes a decision whether to send a domain to the proxy at the DNS layer.
- The DNS request happens before the HTTP/HTTPS connection, which means that when a domain is subject to the proxy, both HTTP and HTTPS traffic is always proxied.
- When HTTP/HTTPS traffic reaches our Intelligent Proxy, the first step is to make a redirect to identify the user.

This redirect is not possible without SSL decryption, which means we might be unable to correctly identify users in some scenarios (such as Roaming Users).

To prevent these users breaking HTTPS requests, Umbrella does not use proxy domains (like eicar.org) that serve both HTTP/HTTPS traffic unless SSL decryption is enabled.

In Summary...

To get the best security and efficacy from the feature, we strongly recommend to install the Cisco Root CA

and enable SSL decryption. This allows eicar.org test files to be blocked and increases the number of domains that are subject to File Inspection through our Intelligent Proxy.

Here is a summary of expected behaviour:

- SSL Decryption OFF
  - Eicar.org sites are **NOT** blocked at https://www.eicar.org/download/eicar.com. The domain is simply not proxied at all because SSL decryption is disabled.
  - Our own test site hosting eicar are blocked: http://proxy.opendnstest.com/download/eicar.com
- SSL Decryption ON
  - Eicar blocked by AV scanning at both http://www.eicar.org/download/eicar.com and https://www.eicar.org/download/eicar.com