How do I manually whitelist a webpage on the Cisco Web Security Appliance (running 5.2.0 and above) so that WBRS, WebRoot or McAfee scanning is bypassed?

TAC **Document ID: 117932**

Contributed by Simon Putz and Siddharth Rajpathak, Cisco TAC Engineers.

Jul 14, 2014

Contents

Question:

Question:

How do I manually whitelist a webpage on the Cisco Web Security Appliance (running 5.2.0 and above) so that WBRS, WebRoot or McAfee scanning is bypassed?

Symptoms:

User is trying to access a legitimate site, but is being blocked due to a low WBRS score (virus infection of webserver, spam being sent through the webserver IP etc.) or due to one of the anti−malware engines triggering on that page.

If the user is blocked due to a low WBRS the user is seeing a MALWARE_GENERAL block message. The accesslogs show a WBRS below the blocking threshold (default is −6.0).

For a permanent solution, please contact Cisco TAC so that the page can be reviewed in order to adjust the WBRS or to report false positives to the anti−virus and anti−malware vendors.

You can also contact Cisco TAC to gather more information on why the site is blocked so that the technical contact or administrator of the website can be notified and can take the necessary steps.
Make sure to provide the relevant blocking codes and accesslog lines when contacting Cisco TAC

To Bypass WBRS:

1. Create a custom URL category containing all sites that you don't want to be blocked (GUI −> Web Security Manager −> Custom URL Categories).
2. Create a new Identity and add the new Custom URL Category as a member. (GUI −> Web Security Manager −> Identities)
   Depending on your setup you will have to choose between 'authentication required' with the according group/user membership settings or 'no authentication'.
3. Create a new Web Access Policy (GUI −> Web Security Manager −> Web Access Policies),

Associate the new Identity with the access policy in the Policy Member Definition.
4. Click on the link in the "Web Reputation and Anti−Malware Filtering" column of your newly created Web Access Policy (it should read 'global policy' until now).
5. Select 'Define Web Reputation and Anti−Malware Custom Settings'
6. Set WBRS scanning to disabled and / or adjust other Malware scanning parameters as required.
7. Submit and Commit your changes.

Note: If you set the action to "Allow" in the URL Category, this would result in bypassing the Anti−Malware/Virus scanning.

To bypass WBRS and anti−malware scanning:

Note: Disabling anti−malware scanning (Webroot and/or McAfee) could be a potential security risk. This should only be done for sites that can be trusted not to contain malware.

1. Create a custom URL category containing all sites that you don't want to be blocked (GUI −> Web Security Manager −> Custom URL Categories).
2. Create a new Identity and add the new Custom URL Category as a member. (GUI −> Web Security Manager −> Identities)
3. Create a new Web Access Policy (GUI −> Web Security Manager −> Web Access Policies), Associate the new Identity with the access policy in the Policy Member Definition.
4. In the new Web Access Policy, where you would like WBRS and Anti−Malware to be bypassed completely, click on the link in the "URL Categories" column.
5. For the Custom URL Category that you have previously created, select the 'allow' action.
6. Submit and Commit your changes.

Updated: Jul 14, 2014 Document ID: 117932